UNIVERSIDAD DE CUENCA

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

ESCUELA DE CONTABILIDAD SUPERIOR Y AUDITORÍA

Elaborar un Plan de Gestión de Riesgos de las Tecnologías de Información y Comunicación basada en el Marco COBIT 5 para Riesgos aplicado a la Universidad de Cuenca

Tesis previo a la obtención del
Título de Contador Público Auditor

AUTORAS:

Daisy Fernanda Alvarado Carpio

Laura Alexandra Zumba Morales

DIRECTOR:

Ing. Paúl Adrián Ochoa Arévalo. MBA, CISA

Cuenca – Ecuador

2015

RESUMEN

El objetivo es la elaboración de un Plan de Mitigación de Riesgos para la Dirección de TIC de la Universidad de Cuenca. Como ente educativo de prestigio debe mantener la vanguardia en la prestación de los servicios académicos para generar profesionales altamente preparados, fundamentándose para ello en: calidad, creatividad e innovación, teniendo a todas las unidades departamentales efectuando actividades de manera óptima y en cumplimiento con normas o reglamentos vigentes.

Por tal motivo, la Gestión de Riesgos enfocada en TIC representa una herramienta esencial para la incorporación de valor y generación de una ventaja competitiva. Su éxito se centra en una adecuada administración. Permite conocer cuáles son los riesgos que afectan a las distintas áreas o unidades del negocio, identificando plenamente vulnerabilidades y amenazas que afecten el cumplimiento de objetivos y regulaciones, evitando de esta manera que los riesgos se materialicen. *COBIT 5 para Riesgos* presenta pautas y estructuras modelos que permiten lograr una óptima gestión de los riesgos al identificarlos, conocerlos, analizarlos y tratarlos.

La aplicación del marco permitirá que los objetivos de la DTIC se efectúen de manera satisfactoria teniendo en cuenta el cumplimiento de la Normativa de Control Interno impartida por la Contraloría General del Estado. Sin embargo, se debe recordar que el marco se considera como una *mejor práctica,* su implementación y adaptación depende de la entidad y su entorno, constituyendo una herramienta de apoyo para el Gobierno Empresarial de TI.

PALABRAS CLAVES: Tecnología de Información y Comunicación (TIC), gestión, riesgos, normativa, óptimo, mitigación.

ABSTRACT

The objective is elaborate a Mitigation Risks Plan for ICT Direction of Cuenca University. As educational entity of prestige it should keep the forefront in its academics services to generate highly trained professionals, all these based on important features such as: quality, creativity and innovation. An important point for that is to have all departments or areas of University doing their activities optimally and in compliance of regulations.

For this reason the Risk Management addressed to ICT is an important essential for adding value and generating a competitive advantage. The successful of it depends the adequate administration. It allows to know the risks that affect to different areas or units of business, identifying vulnerabilities and threats that have negative effects over compliance of goals or external regulations. It prevents risks materialize. In this context COBIT 5 for Risk present guidelines and model structures to achieve an optimal risk management allowing us to identify, know, analyze and treat risks.

The application of this framework will allow to get the ICDT objectives satisfactorily considering compliance of the norm prescribed by the *Contraloría General del Estado*. Nevertheless, you should remember that it is a framework considered as a best practice, its implementation and adaptation depends on the entity and its environment. It is an adaptable tool for supporting IT Enterprise Government.

KEY WORDS: Information and Communication Technology (ICT), management, risks, regulations, optimal, mitigate.

Daisy Fernanda Alvarado Carpio
Laura Alexandra Zumba Morales

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RECONOCIMIENTO DE DERECHOS DE AUTOR

UNIVERSIDAD DE CUENCA
Cláusula de derechos de autor

Yo, DAISY FERNANDA ALVARADO CARPIO, autor/a de la tesis "**Elaborar un Plan de Gestión de Riesgos de las Tecnologías de Información y Comunicación basada en el Marco COBIT 5 para Riesgos aplicado a la Universidad de Cuenca**", reconozco y acepto el derecho de la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de Contador Público Auditor. El uso que la Universidad de Cuenca hiciere de este trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autor.

Cuenca, 23 de abril de 2015.

DAISY FERNANDA ALVARADO CARPIO
C.I: 0104368600

UNIVERSIDAD DE CUENCA
Cláusula de derechos de autor

Yo, LAURA ALEXANDRA ZUMBA MORALES, autor/a de la tesis "**Elaborar un Plan de Gestión de Riesgos de las Tecnologías de Información y Comunicación basada en el Marco COBIT 5 para Riesgos aplicado a la Universidad de Cuenca**", reconozco y acepto el derecho de la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de Contador Público Auditor. El uso que la Universidad de Cuenca hiciere de este trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autor.

Cuenca, 23 de abril de 2015.

Alexandra Zumba

LAURA ALEXANDRA ZUMBA MORALES

C.I: 0105445803

RECONOCIMIENTO DE RESPONSABILIDAD

UNIVERSIDAD DE CUENCA
Cláusula de Propiedad Intelectual

Yo, *DAISY FERNANDA ALVARADO CARPIO*, autor/a de la tesis "**Elaborar un Plan de Gestión de Riesgos de las Tecnologías de Información y Comunicación basada en el Marco COBIT 5 para Riesgos aplicado a la Universidad de Cuenca**", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor.

Cuenca, 23 de abril de 2015.

DAISY FERNANDA ALVARADO CARPIO
C.I: 0104368600

UNIVERSIDAD DE CUENCA
Cláusula de Propiedad Intelectual

Yo, *LAURA ALEXANDRA ZUMBA MORALES*, autor/a de la tesis **"Elaborar un Plan de Gestión de Riesgos de las Tecnologías de Información y Comunicación basada en el Marco COBIT 5 para Riesgos aplicado a la Universidad de Cuenca"**, certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor.

Cuenca, 23 de abril de 2015.

LAURA ALEXANDRA ZUMBA MORALES

C.I: 0105445803

AGRADECIMIENTO

El desarrollo de la presente tesis se ha efectuado durante un tiempo aproximado de siete meses, lapso en el cual varias personas han aportado para su ejecución, es por ello que expresamos nuestros más sinceros agradecimientos a nuestra distinguida y apreciada Universidad de Cuenca en especial a la Directora saliente Ing. Carmita Rojas así como al nuevo Director de la Dirección de Tecnologías de Información y Comunicación el Ing. Patricio Guerrero quienes nos acogieron y facilitaron la información necesaria.

Nuestra mayor gratitud al Ing. Paúl Ochoa por aceptar ser nuestro tutor y director, por su paciencia, comprensión y las recomendaciones dadas que hoy plasmamos en este trabajo.

Por último, a todos nuestros profesores de la Facultad de Ciencias Económicas y Administrativas quienes mediante la formación diaria que nos impartieron contribuyeron a nuestro desarrollo tanto académico como personal, por ser profesores y amigos.

Un sincero *GRACIAS*

Daisy Fernanda Alvarado Carpio

Laura Alexandra Zumba Morales

DEDICATORIAS

Con todo el cariño y amor dedico el logro de mi meta en primer lugar a Dios y a la Virgen Santísima que me conceden el don de la vida y en quienes me encomiendo en todo momento, seguido me complazco en dedicarla a mis padres Tomás y Lorena que me han sabido educar con esmero y dedicación haciendo de mí una mujer responsable y llena de valores, a mi hermana Karla por sus emotivas muestras de afecto y alegría en todo instante.

De manera especial a quién forma parte importante de mi vida, mi enamorado por sus consejos, alientos, recomendaciones y en sí por su gran apoyo incondicional. Es a ustedes a quienes orgullosamente dedico la culminación de mi vida universitaria y la obtención de mi tan anhelado título profesional.

Daisy Fernanda Alvarado Carpio

Dedico este trabajo primeramente a Dios y la Virgencita que iluminaron mi camino para llegar hacia la meta, me dieron una madre que ha sido un pilar fundamental en mi vida y me regalan la oportunidad de estar aquí. Mamá gracias por darme uno de los regalos más importantes en la vida, *el estudio,* gracias a tu esfuerzo, esmero y dedicación hoy soy una profesional; gracias por abrazarme, secarme las lágrimas, celebrar mis alegrías, corregir mis errores; por ti hoy soy una persona hecha y derecha con tu espíritu de seguir adelante y luchar aunque las adversidades sean muchas, a ti por ser la persona más importante te dedico este logro.

A mis abuelitos Manuel y Ermelinda por cuidarme y darme su cariño siempre. A mis padrinos Susy y Hugo así como a sus hijos por ser mi segunda familia. Al Dr. Jorge Peralta por sus consejos y a las amigas que siempre confiaron en mí y estuvieron en todo momento.

Laura Alexandra Zumba Morales

INTRODUCCIÓN

La gestión de riesgos constituye un proceso complejo pero necesario dentro de una entidad, la persona encargada de su diseño e implementación conjuga un sinnúmero de herramientas y conceptos de ramas como: la estadística, matemáticas, auditoría, administración entre otras. El presente documento pretende esquematizar y dar a conocer paso a paso como determinar una metodología de gestión de riesgos aplicada a las Tecnologías de Información y Comunicación de la Universidad de Cuenca.

Se pueden encontrar cuatro capítulos que guardan una relación ordenada y dependencia el uno del otro para ser comprendido de manera integral. En el primer capítulo se aborda información relacionada con el conocimiento general de la entidad ubicando el área relacionada con el manejo de las TIC, los datos obtenidos constituirán la base sobre la cual se efectuará la gestión de riesgos.

En el capítulo siguiente se hace referencia al marco regulatorio que rodea a la Dirección de Tecnologías de Información y Comunicación de la entidad, contemplando normas externas e internas. El capítulo tres presenta una descripción y finalmente una comparación de las mejores prácticas más comunes y reconocidas mundialmente para la Gestión de Riesgos con el objetivo de presentar un bosquejo que permita al lector ubicar a COBIT 5 para Riesgos y entender por qué el modelo brinda efectividad en el tratamiento de riesgos para la entidad.

El último capítulo constituye eminentemente el proceso práctico que conjuga la teoría de los capítulos anteriores con la realidad de la entidad, generando una guía de cómo elaborar el proceso de Gestión de Riesgos de la entidad y obteniendo un matriz de riesgos actuales y residuales de la entidad conjuntamente con propuestas para su tratamiento. En el desarrollo del tema, se emplean términos técnicos por lo cual para comodidad del lector se ha considerado la elaboración de un glosario. Se espera el documento aporte al conocimiento y crecimiento del profesional y demás interesados que lo consulten.

CAPÍTULO I

INFORMACIÓN DE LA INSTITUCIÓN

En este capítulo se pretende conocer de manera general cuál es la razón de ser así como la visión que tiene la Universidad de Cuenca y aquellos valores que le permiten cumplir los aspectos anteriormente mencionados. La entidad para un funcionamiento oportuno y diligente basa sus actividades en procesos dentro de los cuales se puede identificar el accionar de la Dirección de Tecnologías de Información y Comunicación, área en la cual se centra el desarrollo del presente trabajo, ésta se ubica como parte de los procesos habilitantes de apoyo cuyo fin es ser el soporte para cada uno de los procesos restantes de manera que se desarrollen efectivamente. Aquí se detallarán aquellos planes institucionales como: el Plan Estratégico Institucional de la Universidad de Cuenca y el Plan Operativo Anual de la DTIC 2014 datos de utilidad para el análisis de riesgo posterior.

1. INFORMACIÓN INSTITUCIONAL

1.1. Introducción

1.1.1. Misión

La Universidad de Cuenca es una entidad pública, cuya misión es formar profesionales y científicos comprometidos con el mejoramiento de la calidad de vida, en el contexto de la interculturalidad y en armonía con la naturaleza. La Universidad fundamenta en la calidad académica, creatividad e innovación su capacidad para responder a los retos científicos y humanos de la época y sociedad regional, nacional e internacional equitativa, solidaria y eficiente.

1.1.2. Visión

La Universidad de Cuenca se proyecta como una institución con reconocimiento nacional e internacional por su excelencia en docencia con investigación y vinculación con la colectividad; comprometida con los planes de desarrollo regional y nacional; que impulsa y lidera un modelo de pensamiento crítico en la sociedad.

1.1.3. Valores

Compromiso

- Servir a la sociedad y promover la preservación del medio ambiente.
- Cumplir con las regulaciones legales y reglamentarias.
- Apoyar al cumplimiento de las metas del PNBV en lo pertinente a las IES.
- Fortalecer el sentido de identidad y pertenencia aportando proactivamente a las estrategias de mejoramiento institucional.

Transparencia

- Transparentar todos los actos académicos, científicos y administrativos.
- Facilitar el acceso del público a la información institucional.
- Presentar informes y rendir cuentas a la comunidad universitaria y a la sociedad.

Excelencia

- Fomentar e impulsar cambios en la calidad y pertinencia de la educación superior.
- Trabajar bajo los principios de calidad y pertinencia social y científica en el cumplimiento de los ejes misionales.
- Gestionar la excelencia con eficacia y eficiencia.
- Liderar la gestión académica, científica y administrativa.

Lealtad

- Cumplir con la visión, misión y objetivos institucionales aportando a la consecución de las metas del Plan Nacional para el Buen Vivir y al Plan Nacional de Ciencia, Tecnología e Innovación.
- Fomentar el trabajo en Equipo.
- Asegurar una comunicación altamente efectiva hacia dentro y hacia fuera.
- Apoyar a la gestión institucional.

Innovación

- Generar nuevo conocimiento científico y tecnológico.
- Gestionar los cambios institucionales y del entorno con visión proactiva.
- Fortalecer las capacidades y competencias del talento humano.
- Impulsar el desarrollo tecnológico para mejorar la gestión académica y de investigación.

Equidad

- Generar en la comunidad universitaria hábitos de autorreflexión organizacional para promover el cambio.
- Mejorar y diversificar las políticas de acción afirmativa.
- Respetar la diversidad cultural en todas sus manifestaciones y velar por el cumplimiento de los derechos de los diferentes grupos de la comunidad universitaria y de la sociedad. Fortalecer la vinculación con la colectividad.

1.2. Objetivos Institucionales

La Universidad cuenta con objetivos estratégicos por eje misional, enrumbados a Ciencia Tecnología e Innovación, Docencia, Vinculación con la colectividad y Gestión Institucional; para fines de este análisis se han considerado los objetivos estratégicos planteados para el eje de *Gestión Institucional,* los cuales consideran aspectos relacionados con el mejoramiento de la administración de la tecnología informática así como servicios dependientes de la misma.

Los objetivos de la gestión institucional se detallan a continuación:

1. Continuar con el mejoramiento administrativo, tecnológico y físico de los servicios bibliotecarios
2. Actualizar el fondo bibliográfico físico y electrónico.
3. Fortalecer la estructura organizacional de la Dirección de Desarrollo Informático (DDI). (Ahora conocida como DTIC)
4. Automatizar los procesos de la UC.
5. Mejorar progresivamente la calidad de la prestación de servicios informáticos.
6. Mejoramiento de la infraestructura de TIC.
7. Implementar un sistema de planificación institucional.
8. Implementar un proceso de mejora continua en la gestión institucional.
9. Fortalecer los servicios de Bienestar Universitario.
10. Planear el crecimiento físico atendiendo a las necesidades de la docencia, investigación, vinculación con la colectividad y gestión.
11. Reorganizar el staff jurídico para mejorar el asesoramiento a la gestión institucional.
12. Promover el crecimiento integral de las personas potenciando sus capacidades y habilidades.
13. Desarrollar e implantar un nuevo modelo de gestión cultural.
14. Promover la internacionalización de la UC.
15. Implementar un sistema de seguridad física en todos los campus.

16. Mejorar la comunicación institucional interna y externa.
17. Optimizar la gestión financiera.
18. Implementar un proceso de seguimiento financiero y económico al sistema de admisión, matrícula y egreso de estudiantes de pregrado, postgrado y educación continua.

1.3. Estructura Organizacional

En el estatuto institucional se detallan las distintas jerarquías existentes en la institución, es así que los organismos de cogobierno, están formados por el H. Consejo Universitario que es el máximo organismo colegiado académico superior y el H. Consejo Directivo, máximo organismo colegiado de cogobierno de facultad. Dentro de las autoridades de la institución se encuentra a la cabecera el Rector/a que es la máxima autoridad ejecutiva institucional, ejerce la representación legal y extrajudicial además es quien preside el H.C. Universitario en tanto el Vicerrector/a es responsable de las políticas de docencia, investigación y vinculación con la colectividad. Por otra parte las autoridades académicas se refieren a Decanos y Subdecanos, Directores de departamentos, Centros de investigación y programas académicos.

La Universidad de Cuenca posee una estructura organizacional por procesos que permite la total alineación con su misión institucional, ésta estructura se encuentra respaldada en la filosofía y metodología de productos, servicios y procesos con el propósito de asegurar el funcionamiento eficiente, eficaz y efectivo de sus actividades internas orientadas a satisfacer los requerimientos de los usuarios de sus servicios institucionales.

La institución se enfoca en mantener la armonía en sus actividades mediante el establecimiento de procesos como son: procesos gobernantes, procesos que agregan valor y procesos habilitantes, los mismos que en conjunto permiten la elaboración de productos y servicios los cuales se ordenan y clasifican en función de su grado de contribución o valor agregado para alcanzar así su misión institucional.

La formulación y la expedición de políticas, normas e instrumentos que permitan la orientación de la gestión de la institución se encuentran a cargo de los *procesos gobernantes o estratégicos institucionales*.

Los *procesos que agregan valor* son aquellos que generan, administran y controlan los productos y servicios orientados a los usuarios externos y permiten cumplir con la misión institucional.

Los *procesos habilitantes* son aquellos que se focalizan en la generación de productos y servicios de apoyo así como asesoría para los procesos ya mencionados, también pueden valerse a sí mismos encaminando la gestión institucional.

Dentro de los procesos habilitantes *de apoyo* se encuentra la Gestión de las Tecnologías de Información y Comunicación (TIC), cuya existencia y administración es necesaria e indispensable para conseguir una alineación y desempeño óptimo de las actividades en los demás procesos generando así decisiones eficientes que apoyen a la gestión de la institución en general.

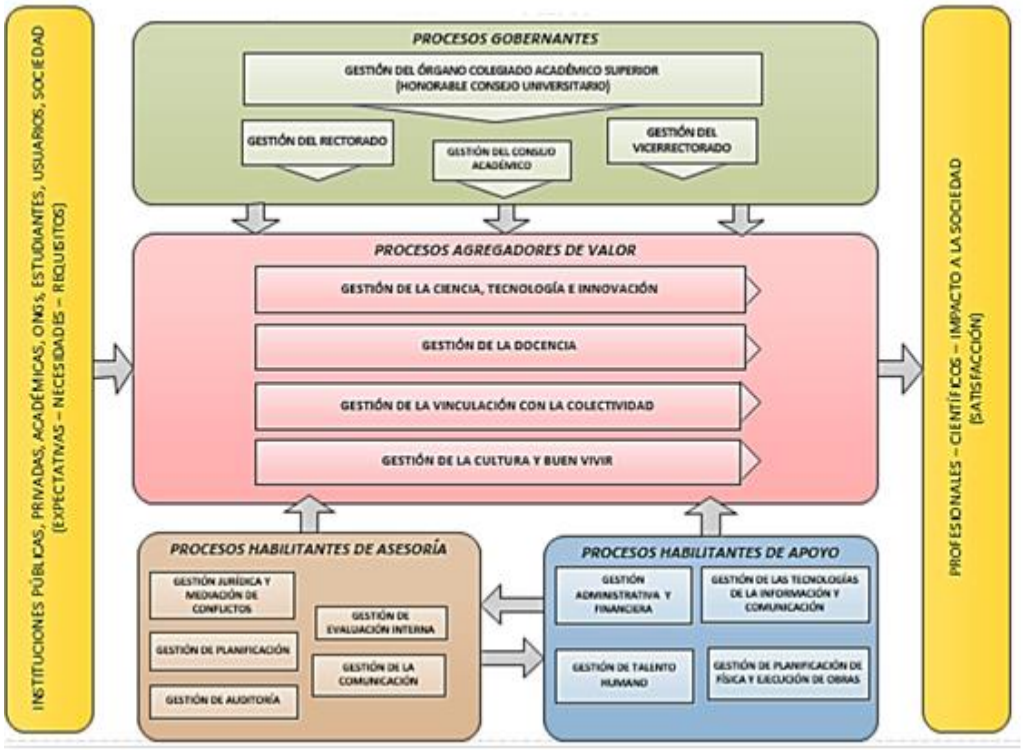


Figura 1 Mapa de Procesos
Fuente: Tomado del Plan Estratégico, Código: UC-DIPUC-PL-09. Vigencia desde: 25-02-2014

1.4. Departamento de Desarrollo Informático

1.4.1. Antecedentes de la Dirección de Tecnologías de Información y Comunicación

Antes del 18 de diciembre del 2013 esta dirección se la conocía como Dirección de Desarrollo Informático (DDI), pero fue modificada con la aprobación del Estatuto de la Institución mediante resolución del Consejo de Educación Superior y actualmente se la conoce como: Dirección de Tecnologías de Información y Comunicación (DTIC).

La DTIC es el órgano administrativo encargado de la gestión, coordinación y ejecución de proyectos en el ámbito de las tecnologías de información y comunicación, su orientación se centra al mejoramiento de la calidad académica y administrativa de la Universidad. Por otro lado, la responsabilidad principal de esta dirección es la operación y mantenimiento de los sistemas de información y de la infraestructura de tecnológica, la seguridad de la información y las instalaciones, y el soporte a usuarios.

Actualmente la DTIC posee tres coordinaciones: Sistemas de Información, Redes y Comunicaciones, y Servicios Informáticos.

1. **Coordinación de Sistemas de Información.-** Se encarga de dotar y administrar sistemas de información innovadores y con calidad, que automaticen los procesos de manera que contribuyan a la consecución de los objetivos institucionales.

2. **Coordinación de Redes y Comunicaciones.-** Se encarga de proporcionar una infraestructura tecnológica robusta y de la más alta calidad así como suministrar servicios de comunicaciones eficientes y eficaces que ayuden a satisfacer las necesidades informáticas institucionales.

3. **Coordinación de Servicios Informáticos.-** Se encarga de brindar, promover, coordinar y evaluar los servicios de Sistemas de información y Comunicación, en las unidades administrativas, académicas y de investigación de la Universidad de Cuenca, procurando la mejora continua de estos servicios y su alineamiento con las necesidades de la comunidad universitaria.

Cada año la DTIC elabora su Plan Operativo Anual (POA) con el objeto de alinear sus actividades al desarrollo estratégico de la Institución. El POA 2014

de la DTIC está basado en el *Plan Estratégico Institucional de la Universidad de Cuenca (PEUC) 2012 -2017*, en el *Plan de Mitigación de Riesgos de la institución 2012*, y en las *Recomendaciones del Informe de evaluación integral del Sistema de Control Interno* realizado por la Unidad de Auditoría Interna.

1.4.2. Misión

La Dirección de Tecnologías de Información y Comunicación, es el órgano encargado de la gestión, coordinación y ejecución de proyectos en el ámbito de las tecnologías de información y comunicación, orientados al mejoramiento de la calidad académica y administrativa de la Universidad.

1.4.3. Objetivos de la DTIC

Los objetivos que persigue la dirección de TIC están definidos en el PEUC vigente y son:

1) Fortalecer la estructura organizacional de la Dirección de Desarrollo Informático (ahora DTIC).
2) Automatizar los procesos de la Universidad de Cuenca.
3) Mejorar progresivamente la prestación de servicios informáticos.
4) Mejora de la infraestructura de tecnologías de información y comunicación.

1.4.4. Funciones

Son funciones de la Dirección de Tecnología de Información y Comunicación:

a) Proponer proyectos en el campo de las tecnologías de información y comunicación que procuren la calidad académica y administrativa de la Universidad, y establecer políticas universitarias de uso de las tecnologías de información y comunicación.
b) Asesorar a los organismos de gobierno universitario en la implementación de sistemas de información y nuevas tecnologías en los procesos académicos, de investigación y de gestión.
c) Incentivar, asesorar, coordinar y apoyar el uso de la informática en Facultades, Departamentos y demás unidades académicas, promover la

cultura del cuidado, conservación, eficiencia y buen uso de los equipos y sistemas informáticos.

d) Investigar e implementar nuevas tecnologías de información y comunicación que faciliten los procesos universitarios; planificar, evaluar y dar seguimiento a la implementación de sistemas informáticos integrales que permitan modernizar y agilitar los procesos académicos y administrativos.
e) Diseñar, implementar y mantener los sistemas de información de la Universidad empleando nuevas tecnologías de desarrollo de software.
f) Implementar, administrar, mantener la red de datos y comunicación universitaria interna y externa.
g) Responder por el buen funcionamiento de los servidores centrales, equipos de comunicaciones, almacenamiento, procesamiento y acceso a la información institucional.
h) Administrar el centro de datos, desarrollar procesos de operación en coordinación con las unidades que usen este servicio y las demás que le confieran el Estatuto y los reglamentos de la Universidad de Cuenca.

1.5. Plan Estratégico

1.5.1. Plan Estratégico Institucional

1.5.1.1. Marco Legal

El Plan Estratégico de la Universidad de Cuenca tiene tres referentes máximos a los cuales se debe alinear y responder, según su jerarquía tenemos:

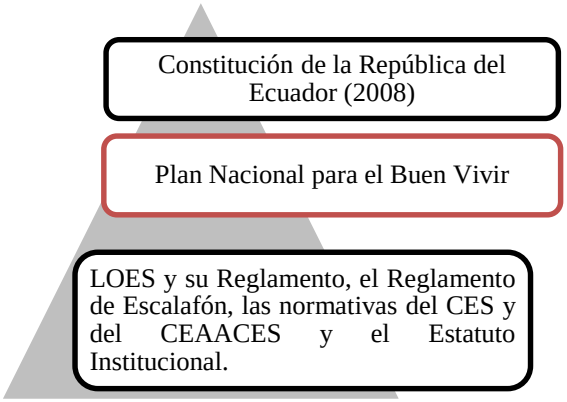


Figura 2 Jerarquía Legal
Fuente: Plan Estratégico de la Universidad de Cuenca 2014, Código: UC-DIPUC-PL-09

La Constitución de la República constituye la base legal del plan, mientras que la base política administrativa se define en la segunda parte de la pirámide por último en la parte baja se ubica la base institucional y de concreción de la política pública sectorial.

1.5.1.2. Objetivos Estratégicos de Desarrollo Institucional

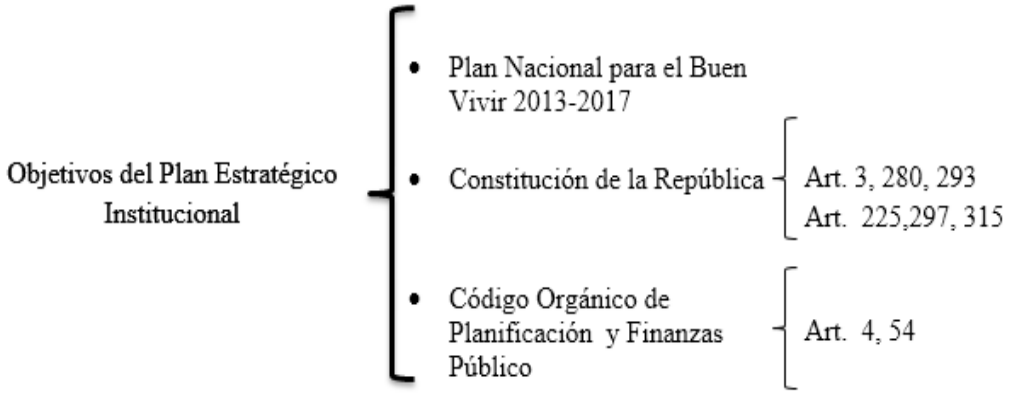


Figura 3 Esquema de Leyes
Fuente: Plan Estratégico de la Universidad de Cuenca 2014, Código: UC-DIPUC-PL-09

La educación constituye un pilar fundamental para lograr que la ciudadanía se desarrolle en un ambiente de BUEN VIVIR o Sumak Kawsay donde sus derechos primordiales se respeten y a la vez cumplan con las responsabilidades como ciudadanos de la nación.

Con este fin se desarrolló el Plan Nacional del Buen Vivir, en el cual se determinan los objetivos para alcanzar dicho propósito, la elaboración del Plan Estratégico Institucional de la Universidad de Cuenca se fundamenta en el cuarto objetivo de este plan *"Fortalecer las capacidades y potencialidades de la ciudadanía"* así como en algunas de sus políticas centradas en calidad, interacción y espacios para la educación.

La universidad como entidad del sector público creada para la prestación de un servicio público, se sujeta a determinados artículos de la Constitución de la República del Ecuador así como el Código Orgánico de Planificación y Finanzas Públicas. Se alinea principalmente a los artículos constitucionales en los cuales se menciona a la educación como un deber primordial del Estado pero teniendo en cuenta la vinculación con otros deberes que en conjunto generen bienestar en la población.

Se puede rescatar que todos los planes, programas y proyectos públicos se deben subordinar a lo que se encuentra establecido en el Plan Nacional de Desarrollo, por ello la institución debe priorizar sus necesidades, de modo que pueda cumplir con sus objetivos, cuidándose de esta manera de no caer en el error de planear desmesuradamente. Esto conlleva a que la institución defina un plan estratégico muy bien trabajado donde se vislumbren todas las metas, con periodos de tiempo así como métricas para su evaluación, que permita cumplir su visión institucional pero también es necesaria la alineación de cada una de las unidades que conforman la universidad de manera que el trabajo sea conjunto con mira hacia un solo objetivo; por lo tanto las definición de actividades o proyectos de cada unidad debe estar conforme a lo que la institución como tal quiere lograr.

A continuación, se presenta un esquema de los objetivos estratégicos establecidos a nivel de toda la institución, cabe mencionar que únicamente se han definido en su totalidad los objetivos por eje misional respecto a la Gestión Institucional, ya que aquí se hallan los objetivos que son de interés y base del presente trabajo.

OBJETIVOS ESTRATÉGICOS	OBJETIVOS	
Razón de ser la entidad	Incrementar en un 200% la publicación de artículos científicos y tecnológicos en revistas indexadas como plataforma para convertir a la UC en una institución de educación superior generadora de ciencia, tecnología e innovación para el desarrollo de la región y el país al 2017.	
	Incrementar la eficiencia terminal de grado y posgrado formando profesionales altamente cualificados que contribuyan al cambio de la matriz productiva y al desarrollo social, con capacidades de generar y transferir conocimiento en el campo de la investigación básica y aplicada.	
	Incrementar la participación de la UC en el cambio de la matriz productiva zonal y nacional mediante la ejecución de programas y proyectos en convenio con el Estado, las comunidades y los sectores productivos, integrando los saberes ancestrales, económicos y ambientalmente sostenibles y sustentables.	
	Incrementar el nivel de excelencia del servicio brindado al usuario.	
OBJETIVOS ESTRATÉGICOS	**OBJETIVOS**	**OBJETIVOS ESTRATÉGICOS POR EJE MISIONAL**
Fortalecimiento Institucional	Convertir a la UC en una institución de educación superior generadora de ciencia, tecnología e innovación, en tres direcciones complementarias: (1) Incrementando el nivel de soporte a la matriz productiva y al desarrollo social dedicando un mayor esfuerzo al diseño y ejecución de proyectos de investigación zonal, (2) Incrementando la cooperación a nivel nacional, regional e internacional en redes de excelencia de investigación y (3) Incrementando la publicación de artículos científicos en revistas indexadas.	Ciencia, Tecnología e Innovación
	Incrementar progresivamente el número de docentes con título de PhD con perfiles orientados al cambio de la matriz productiva y al desarrollo	Docencia

		social, con capacidades de generar y transferir conocimiento en el campo de la investigación básica y aplicada de acuerdo a los intereses estratégicos del país.		
		Incrementar el nivel de vinculación con la colectividad acorde al nuevo modelo de generación y gestión del conocimiento.	Vinculación a la colectividad	
	Fortalecimiento Institucional	Incrementar el nivel de eficiencia de la gestión académica y administrativa acorde al nuevo modelo de generación y gestión del conocimiento y del modelo de gestión por procesos.	**Gestión Institucional**	Continuar con el mejoramiento administrativo, tecnológico y físico de los servicios bibliotecarios.
				Actualizar el fondo bibliográfico físico y electrónico
				Fortalecer la estructura organizacional de la Dirección de Desarrollo Informático (DDI
				Automatizar los procesos de la UC.
				Mejorar progresivamente la calidad de la prestación de servicios informáticos.
				Mejoramiento de la infraestructura de TIC.
				Implementar un sistema de planificación institucional.
				Implementar un proceso de mejora continua en la gestión institucional.
				Fortalecer los servicios de Bienestar Universitario.
				Planear el crecimiento físico atendiendo a las necesidades de la docencia, investigación, vinculación con la colectividad y gestión
				Reorganizar el staff jurídico para mejorar el asesoramiento a la gestión institucional
				Promover el crecimiento integral de las personas potenciando sus capacidades y habilidades.
				Desarrollar e implantar un nuevo modelo de gestión cultural.
				Promover la internacionalización de la UC.
				Implementar un sistema de seguridad física en todos los campus.
				Mejorar la comunicación institucional interna y externa
				Optimizar la gestión financiera.
				Implementar un proceso de seguimiento financiero y económico al sistema de admisión, matrícula y egreso de estudiantes de pregrado, postgrado y educación continua.

Considerados ***objetivos estratégicos*** de DTIC

Figura 4 Plan Estratégico Institucional
Fuente: Plan Estratégico de la Universidad de Cuenca 2014, Código: UC-DIPUC-PL-09

1.5.2. Plan Operativo Anual 2014 de la Dirección de Tecnologías de Información y Comunicación

OBJETIVOS ESTRATÉGICOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN (TIC)	PROYECTOS
1. **Fortalecer la estructura organizacional de la DDI (ahora DTIC)**	Plan de Capacitación del Personal de TIC
	Implementación de la Metodología para el desarrollo, mantenimiento y/o adquisición de software y estructura del Centro de Desarrollo de Software
2. Automatizar los procesos de la Universidad de Cuenca.	Elaborar un Banco de proyectos de software priorizados
	Autenticación única para acceso a los sistemas y servicios informáticos.
	Sistema de Gestión Académica de Postgrados II Fase E – SGAP Centro
	Integración del Repositorio de publicaciones con el Portafolio Centro
	Integración de sitios web para móviles con los sistemas de la Universidad
	Sistema de Estadísticas Institucionales
	Mejoras en el Sistema de Gestión de Investigación – SGI
	Finalizar adecuación de los Sistemas Informáticos para el cambio de identificación única de las personas.
	Renovación de equipos para el personal
	Implementación del Sistema de Gestión Institucional (Open ERP)
	Sistema de Gestión de Cursos de Educación Continua
	Sistema de Gestión de Seguimiento de Graduados - SGG
	Sistema de Gestión de TIC
	Sistema de Gestión de Vinculación
	Sistema de Gestión de Proyectos
	Mejoramiento del Rendimiento de la Base de Datos y Servidores de Aplicaciones
	Administración de sistemas y soporte especializado a usuarios de sistemas académicos
	Administración de sistemas y soporte especializado a usuarios de sistemas administrativos y financieros
	Compra de licencias de archivos PDF y Control de fechas
	Plan de capacitación a usuarios en el uso de los sistemas de información
3. Mejorar progresivamente la prestación de servicios informáticos	Sistema de control de acceso y seguridad física de la DTIC
	Implementación de un sistema de almacenamiento y gestión de documentación institucional con ALFRESCO
	Creación de un clúster de servidores para la prestación del servicio de portales Web institucionales
	Creación de un clúster de servidores para la prestación del servicio del entorno Virtual de Educación
	Integración de la Plataforma de Aprendizaje Virtual - eVirtual con el Sistema de Gestión Académica
	Capacitación para administración de Servicios de Redes y Comunicaciones
	Generación de usuarios para docentes y empleados que se integran a la Universidad
	Capacitación a usuarios en el manejo de Sistemas de Información y utilitarios

	Implementación del Sistema de Voto Electrónico en procesos electorales
	Realizar encuestas con la Aplicación LimeSurvey
	Migración y Actualización del Antivirus en el Servidor Principal y Secundarios
	Implementar software de Gestión de Servicios de la DTIC
4. Mejorar de la infraestructura de tecnologías de información y comunicación	Elaboración y ejecución de procedimiento de evaluación de los servicios informáticos
	Adquisición e implementación de equipo Antispam
	Adquisición de una Librería de cintas adicional para respaldos de información
	Implementación de un Anillo de Fibra Óptica para el Campus Central
	Adquisición de rack, switches y patch pannel
	Adquisición de infraestructura de servidores para el Centro de Datos
	Adquisición de infraestructura de almacenamiento común para el Centro de Datos
	Adquisición de UPS redundante para Centro de Datos
	Adquisición de computadores para personal de Redes y Comunicaciones
	Ampliación de la Red inalámbrica universitaria
	Implementar el equipamiento informático en el Nuevo Centro de Computo de las Facultades de Filosofía, Jurisprudencia, Psicología e Idiomas
	Sistema de respaldos de información de usuarios finales
	Cambio de computadoras y equipos de la CSE
	Implementación del Sistema de Gestión de Incidentes de seguridad informática
	Implementación de Sensores y Honeypots para captura de tráfico no permitido
	Implementación de seguridad perimetral de la red de datos
	Aseguramiento de red UCWIFI
	Mejora y aseguramiento de red Dual Stack.

Figura 5 Plan Operativo de la DTIC
Fuente: Plan Operativo Anual de la DTIC de la Universidad de Cuenca– POA 2014

En la figura 5 se presenta los objetivos estratégicos con sus respectivos proyectos, de manera general, independientemente de la coordinación a cargo de su realización y administración, no se han detallado las actividades a llevarse a cabo ya que no se consideran relevantes para el desarrollo del trabajo.

CAPÍTULO II

MARCO REGULADOR

En este capítulo se pretende explicar las regulaciones tanto internas y externas a las cuales se encuentra sujeta la DTIC de la Universidad de Cuenca, considerando dentro de las internas el estatuto y las políticas de tecnología, mientras que en las externas está el marco de control interno que debería tener la Universidad para cumplir con la normativa, también se detallan ciertos aspectos relacionados con la Contraloría y el marco integrador COSO; con el fin de enlazar los conceptos.

Daisy Fernanda Alvarado Carpio
Laura Alexandra Zumba Morales

2. MARCO REGULADOR

2.1. Antecedentes

La Universidad de Cuenca como entidad pública maneja recursos públicos razón por la cual se encuentra bajo la supervisión de entes fiscalizadores entre, los cuales, se ubica la Contraloría General del Estado, organismo que ha desarrollado y emitido normativa que rige el control interno.

La observancia de las leyes emitidas respecto al Control Interno es obligatoria, le permitirá a una entidad lograr eficiencia y eficacia en sus operaciones para la consecución de los objetivos previamente establecidos, actuando dentro de un marco limitante. La normativa fue desarrollada en base al marco COSO distinguiendo varias premisas o normas específicas para cada uno de los componentes.

2.2. Marco Interno

2.2.1. Estatuto

En este se detalla las diferentes delegaciones y funciones de cada uno de los departamentos, unidades, direcciones y demás que forman parte de la universidad, para el análisis posterior se consideran aquellos que son significativos y que aportan a los fines que busca este trabajo.

A continuación, se dará a conocer de manera sintetizada las principales funciones administrativas, que sirven como una base de conocimiento para entender el medio en el cual se realizan las actividades generales de las cuales es dependiente la DTIC.

ÁREAS	FUNCIONES
CONSEJO UNIVERSITARIO Art. 17	i) Conocer y aprobar el Plan Estratégico que eleve a su consideración el Rector. El plan deberá estar en concordancia con el Plan Nacional de Ciencia y Tecnología, Innovación y Saberes Ancestrales y el Plan Nacional de Desarrollo. j) Conocer y aprobar anualmente en el Plan Operativo y el Presupuesto de la Universidad, propuesto por el rector, en el que debe constar obligatoriamente el 6% para publicaciones indexadas, becas de posgrados para los profesores e investigadores y año sabático; y, el 1% del Presupuesto Institucional Anual para la formación y capacitación de los profesores e investigadores contemplado en el art. 28 del Reglamento General de la LOES. k) Conocer y aprobar los gastos, inversiones, enajenaciones y donaciones que eleve a su consideración el Rector, de conformidad con la ley.
RECTORADO Art. 21	a) Cumplir y hacer cumplir la Constitución de la Republica, la Ley Orgánica de Educación Superior, su Reglamento, los reglamentos y resoluciones del Consejo de Educación Superior, el Estatuto, las disposiciones generales y las resoluciones del Consejo Universitario. d) Presentar el reglamento de la estructura orgánica y funcional administrativa de la Universidad al Consejo Universitario para su aprobación y expedir los manuales e instructivos respectivos para su mejor aplicación. g) Elevar a conocimiento y aprobación del Consejo Universitario el Plan Estratégico, Plan Operativo, el presupuesto, los gastos, inversiones, enajenaciones y donaciones de conformidad con la ley y el Estatuto.
DIRECCIÓN DE PLANIFICACIÓN Art. 24	a) Desarrolla el proceso de planificación universitaria alineándose con el Plan Nacional de Desarrollo, y articulada con el Sistema Nacional de Educación Superior, Ciencia y Tecnología. b) Realizar acompañamiento a la elaboración e implementación de planes operativos académicos y administrativos en las facultades y dependencias. d) Elaborar el banco de estadísticas con información académica y administrativas. e) Planificar el desarrollo informático de la universidad en relación con los procesos académicos, administrativos, financieros, de recursos humanos y materiales, en coordinación con la Dirección de Tecnologías de la Información y Comunicación.
CONSEJO ACADÉMICO Art. 53	n) Asesorar al Consejo Universitario y a las autoridades de la universidad en las áreas de su competencia.
VICERRECTORADO Art. 47	a) Compartir con el rector la responsabilidad académica y administrativa de la universidad. b) Presidir o integrar los organismos de conformidad con el presente Estatuto y los reglamentos, y ejercer las delegaciones y atribuciones conferidas por el Rector.
SERVIDORES Y TRABAJADORES Art. 109-110-112	Principales derechos: d) La participación y cumplimiento de las disposiciones legales, estatutarias y reglamentarias. e) El estímulo a su permanente mejoramiento personal, técnico, científico y cultural. f) La mejora constante de sus conocimientos y capacidades profesionales. Principales obligaciones: b) Cumplir las tareas atinentes a su cargo con oportunidad, responsabilidad, cortesía y eficiencia. c) Acatar las disposiciones emanadas de las autoridades universitarias. d) Guardar la debida reserva sobre la información, datos, documentos y resoluciones siempre y cuando dicha reserva no constituya una restricción injustificada al derecho al acceso a la información. Los requisitos para ser servidor o trabajador de la Universidad de Cuenca e establecerá en el reglamento respectivo.

Figura 6 Funciones de los departamentos, unidades o direcciones institucionales
Fuente: Estatuto de la Universidad de Cuenca

2.2.2. Política de TI

POLÍTICAS DE TECNOLOGÍA								
GENERALES	DE DATOS	DE ACTIVOS TECNOLÓGICOS Y EQUIPOS INFORMÁTICOS	DE PROGRAMAS INFORMÁCTICOS	DE SEGURIDAD	DE ACCESO	DE COMUNICACIONES CONVERGENTES	DE TELECOMUNICACIONES	DE INTERNET Y CORREO ELECTRÓNICO
Aspectos Generale	Propiedad y privacidad	Uso	Uso	Seguridad de la Información	Perfiles de usuario	Redes sociales	Telecomunicaciones	Uso
Gestión tecnológic	Uso	Adquisición	Adquisición	Vigilancia y retenci	Contraseñas		Telefonía	Datos
Comité de TIC	Almacenamiento	Almacenamiento	Licenciamiento	Confidencialidad	Acceso físicos			
Acuerdos del nivel de servicio				Integridad de datos				
				Disponibilidad				
				Medidas y preventivas y de contención				

Figura 7 Políticas de TI
Fuente: Política de Tecnología de la Universidad de Cuenca CODIGO: UDC-DTIC-CSE-04

Las políticas dentro de una institución son imprescindibles, ya que delimitan lo que se debe y no realizar dentro de la institución, para su correcta adopción y cumplimiento por parte de las personas involucradas requiere de una adecuada divulgación y comunicación. A continuación se detalla las políticas definidas para la DTIC (DTIC, Ingeniero de Sistemas, 2014):

Políticas generales.- Orientadas a todos los usuarios que interactúan con la tecnología de la información, pudiendo ser estos activos o concurrentes dentro de los cuales pueden estar los estudiantes, docentes, unidades académicas y administrativas, entre otros; los mismos que demandan optimización en las operaciones diarias. Estas políticas establecen que para una adecuada gestión tecnológica se considerará el uso de marcos metodológicos para la gestión de proyectos así como de prácticas mundialmente aceptadas para el control, gestión y gobierno.

Por otro lado se menciona la incorporación de un Comité de TIC que se encargue de la planeación y toma decisiones estratégicas en pro de la universidad y por último, se incluye la coordinación de los acuerdos de nivel de servicio entre los usuarios y el área de servicio, buscando de esta manera la satisfacción total de los mismos de manera equilibrada.

Políticas de datos.- Consideran la ética, confidencialidad y buen uso de la información, la cual se clasifica como pública y cuya propiedad según las leyes y reglamentos existentes le corresponde a la Universidad de Cuenca, por tal motivo estas políticas establecen la definición de perfiles de acceso para conocer a los responsables de la custodia o protección de los datos, teniendo en cuenta que el uso de los mismos será regulado mediante acuerdos de uso y confidencialidad. En cuanto al almacenamiento la DTIC se preocupará de la integridad, disponibilidad y respaldo de los mismos mediante bases de datos adecuadamente administradas.

Políticas de activos tecnológicos y equipos informáticos.- Hacen referencia al uso, cuidado y tratamiento tanto para la adquisición como renovación de los activos y equipos informáticos según los avances tecnológicos. Dentro de estas políticas se establece que los equipos tecnológicos e informáticos serán empleados según las necesidades de la universidad, es por ello que para su adquisición se debe tener en cuenta la marca y la garantía de los mismos mientras que para su alquiler la DTIC analizará los beneficios de optar por esta opción. Por otro lado, para el reemplazo se deberá considerar los siguientes requisitos: que no cumpla con las características técnicas o este dañado y el costo sea superior al 50% del valor de adquisición.

Políticas de programas informáticos.- En estas se detalla que los programas o sistemas informáticos adquiridos o desarrollados tendrán como fin el cumplimiento de los objetivos institucionales los cuales se encuentran vinculados con las actividades de los funcionarios quienes estarán a cargo del manejo de estos programas. Se deberá tener en cuenta que todo software empleado en la universidad debe poseer o se solicitará su respectivo licenciamiento de tipo académico; la DTIC llevará un registro de todo el software adquirido con el fin de evitar repetición.

Políticas de seguridad.- Implican alineamientos para proteger la información tanto de ataques internos o externos, es por ello que en estas se estipula la asignación de las responsabilidades, derechos y obligaciones que debe tener un

usuario considerando que la seguridad de la información es responsabilidad de todos los involucrados, por lo cual se requiere una reserva asegurada adecuadamente de los datos así como la definición de criterios para considerar a una información como confidencial, mientras que para mantener la integridad de los datos se plantea el impedimento de su manejo por parte de personas no delegadas así como del uso de herramientas de software y hardware. Dentro de esta política se indica que se evitará cualquier interrupción de los sistemas garantizando así la disponibilidad de los mismos lo cual es responsabilidad de la DTIC.

Políticas de acceso.- Son aquellas diseñadas con el fin de lograr la integridad de los equipos, datos y servicios entregados a través de la determinación por parte de la DTIC de los derechos y restricciones, tanto para el acceso a la información como para lugares físicos internos o externos definidos como zonas restringidas. También se encargará de fomentar el uso de contraseñas complejas las cuales se caracterizan por ser digitalizadas, poseer al menos una letra mayúscula, minúscula y un carácter; evitando colocar cualquier dato personal en las mismas.

Políticas de comunicaciones convergentes.- Se detallan los lineamentos para un uso idóneo de las diferentes redes sociales en las cuales se resalta que las mismas serán empleadas únicamente con fines informativos, académicos y administrativos aprovechando así las ventajas que brindan las innovaciones tecnológicas.

Políticas de telecomunicaciones.- Consideran la relación que debe tener la DTIC con las diversas dependencias de la universidad con el fin de que ésta pueda conocer y asesorar la instauración y mejoramiento de las líneas de comunicación necesarias para obtener calidad en la red de datos. Estas políticas incluyen pautas para el acceso y funcionamiento de la telefonía usada por los distintos usuarios autorizados.

Políticas de internet y correo electrónico.- Son aquellas a través de las cuales se regulariza el uso de estas herramientas consideras de apoyo para la

comunidad universitaria, la DTIC se encargará de difundir el uso del correo electrónico asegurando que la información enviada y recibida es confidencial; además se establecerán los criterios para el almacenamiento, eliminación y recuperación de la información encontrada en el buzón.

2.3. Marco externo

2.3.1. Contraloría General del Estado

En Ecuador, esta institución se instauró el 2 de diciembre de 1927, dedicada a fiscalizar las actividades administrativas así como las referentes a los presupuestos de todas las instituciones que conforman el sector público o poseen recursos públicos. Conjuntamente con tres entidades más, conforman el cuarto poder denominado Función de Transparencia y Control Social.

Según consta en la Constitución, esta entidad es un organismo técnico encargado del control de la utilización de los recursos estatales, y la consecución de los objetivos de las instituciones del Estado y de las personas jurídicas de derecho privado que dispongan de recursos públicos. (Constituyente, 2008)

2.3.1.1. Misión

La razón de ser de la institución es controlar los recursos públicos para precautelar su uso efectivo, en beneficio de la sociedad.

2.3.1.2. Visión

Respecto a su proyección se plantea ser reconocida como un referente de excelencia en el control de los recursos públicos.

2.3.1.3. Funciones

Se establecen como funciones de la Contraloría las siguientes:

- Dirigir el sistema de control administrativo que se compone de auditoría interna, externa y del control interno de las entidades del sector público y de las entidades privadas que dispongan de recursos públicos.

- Determinar responsabilidades administrativas y civiles culposas e indicios de responsabilidad penal, relacionadas con los aspectos y gestiones sujetas a su control, sin perjuicio de las funciones que en esta materia sean propias de la Fiscalía General del Estado.

- Expedir la normativa para el cumplimiento de sus funciones.

- Asesorar a los órganos y entidades del Estado cuando se le solicite. (Constituyente, 2008)

Dentro de la normativa expedida tenemos las: Normas de Control Interno para entidades organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos, que serán objeto de análisis en los párrafos siguientes.

2.3.2. Normas de Control Interno para entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos.

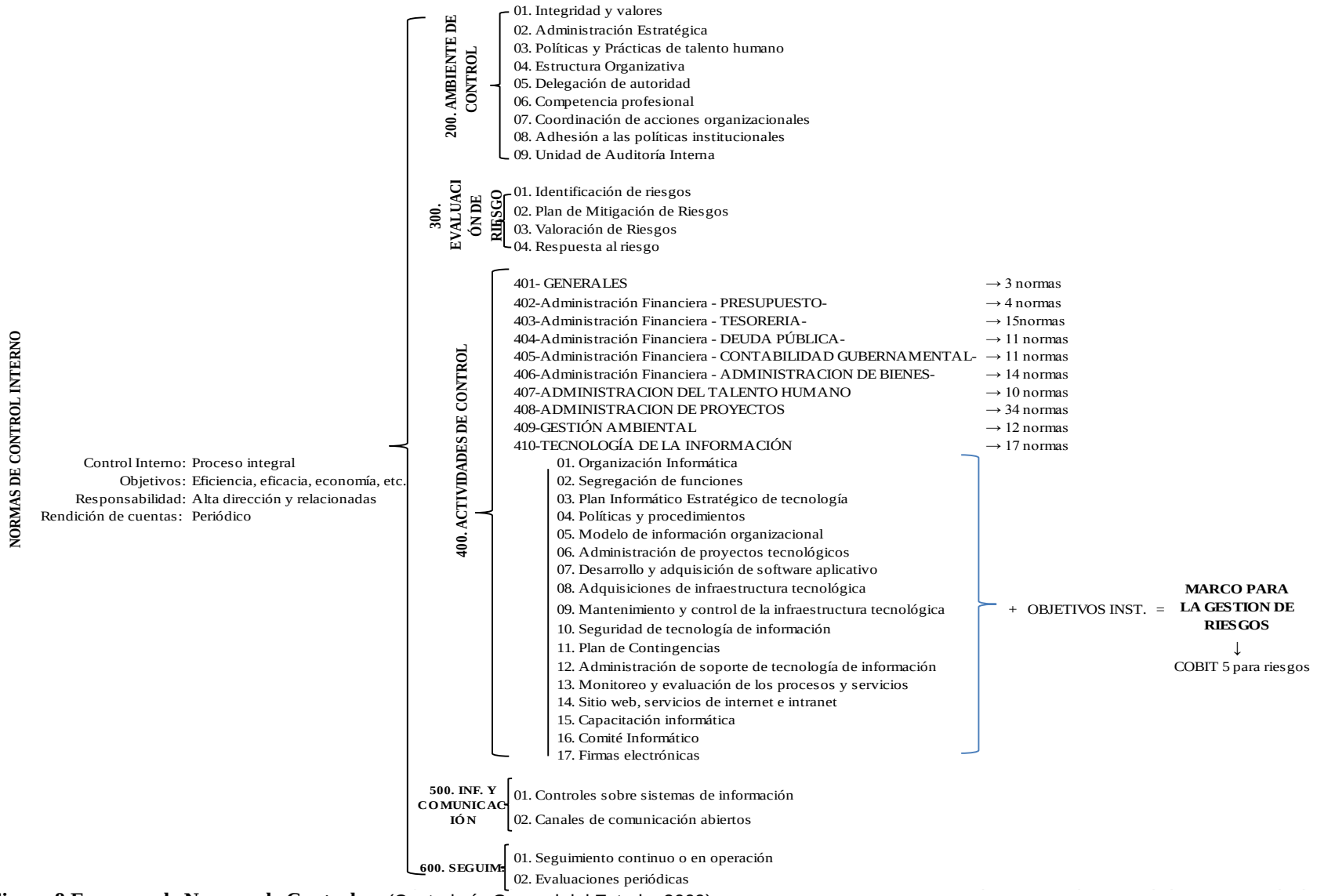
La Contraloría General del Estado emitió las Normas de Control Interno para entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos, en cumplimiento de sus funciones, mediante el acuerdo 039-CG-2009 dando de baja a las emitidas mediante acuerdo 020-CG-2002 y registradas el 10 de octubre del mismo año. Esto obedeció a los cambios que se estaban dando en el manejo de las actividades a nivel global por lo que se consideró necesaria una actualización.

Según el acuerdo 006-CG-2014 se reformó la sección 408 referente a la Administración de Proyectos, agregando un campo más, anteriormente se manejaba hasta 408-33 *Evaluación Ex-post* a ello se incorpora el campo 408-34 *Consultoría.*

También bajo el acuerdo 052-CG-2014 se reformó la sección 406 referente a Administración de bienes, agregando la norma 406-14 *Bienes procedentes de regalos o presentes de tipo institucional.* Estos cambios, según la designación de la contraloría, la actualización está a cargo de La Dirección de Investigación Técnica, Normativa y de Desarrollo Administrativo de la Contraloría General del Estado.

Esta normativa utiliza como base los cinco componentes del COSO según consta en el documento de presentación de la normativa en el párrafo tercero: " *Las normas de control interno desarrolladas incluyen: normas generales y otras específicas relacionadas con la administración financiera gubernamental, talento humano, tecnología de la información y administración de proyectos y recogen la utilización del marco integrado de control interno emitido por el Comité de Organizaciones que patrocina la Comisión Treadway (COSO), que plantea cinco componentes interrelacionados e integrados al proceso de administración, con la finalidad de ayudar a las entidades a lograr sus objetivos."*

Sin embargo, para el análisis correspondiente se tomará como referencia únicamente la sección de las *actividades de control* en al cual se destina una sección al tratamiento de temas relacionados a las tecnologías de información.



Fuente:

Figura 8 Esquema de Normas de Control (Contraloría General del Estado, 2009)

2.3.2.1. Norma 300: Evaluación del Riesgo

La Universidad cuenta con un Plan de Mitigación de Riesgos enfocado en la estructura general dentro del cual se contemplan varios riesgos, donde algunos de estos afectan de manera significativa a la DTIC en cumplimiento a la norma 300-02 *Plan de mitigación de riesgos*. Dicha norma establece que toda entidad pública deberá implementar planes acordes a sus necesidades que permitan el aseguramiento y protección de sus recursos.

En general, esta norma detalla las pautas a seguir para un adecuado y eficaz control de riesgos empezando por su identificación y continuando con un plan de mitigación, valoración y respuesta a los mismos. Esta norma es la actualmente aplicada por la entidad.

Sin embargo, la Universidad de Cuenca y en especial la DTIC maneja procesos que en su totalidad son automatizados por lo cual se encuentra sujeta a una mayor cantidad de riesgos tecnológicos por dicho motivo requiere apoyarse en una norma específica que direccione dichas actividades de tratamiento de riesgo permitiéndole así lograr una eficiencia en sus acciones y servicios.

2.3.2.2. Norma 410: Tecnologías de la Información

El desarrollo del tema se centra en el componente *Actividades de Control* (grupo de las 400) dentro de las cuales la norma 410 menciona los lineamentos que deben regir para la TECNOLOGÍA DE LA INFORMACIÓN dentro de la institución, por ello se deberá tomar en cuenta una adecuada organización informática en la cual se establece la segregación de funciones que permitan ejercer las actividades con suficiente autoridad y respaldo, soportadas con un plan informático estratégico de tecnología que este en concordancia con el plan estratégico institucional, para lo cual es necesario establecer políticas y procedimientos, así como también un modelo de información organizacional que delimite el marco de trabajo.

Esta normativa provee mecanismos para la administración de proyectos tecnológicos que faciliten su gestión, teniendo en cuenta aspectos importantes para el desarrollo y adquisición de software o infraestructura tecnológica. Por otra parte, se recalca la importancia sobre la seguridad de la tecnología de la información dentro de los cuales se toma en cuenta los planes de contingencia, así como la administración de soporte de tecnología de la información, monitoreo y evaluación de los procesos y servicios.

Por último, plantea la elaboración de normas, procedimientos e instructivos para manejo de los sitio web, servicios de internet e intranet para lo cual se necesita una capacitación informática y el establecimiento de un comité informático.

Los aspectos relevantes de la normativa a cumplir referente al control interno, que se rescatan, se detallan a continuación:

a) La función a desempañar el área de TI (DTIC) debe cubrir las funciones de *asesoría y apoyo,* esto sin duda, es vital para que la entidad pueda obtener valor agregado de sus actividades. De esta función pueden beneficiarse los altos directivos así como los usuarios. Se considerará entonces importante la presencia de delegados o representantes del área en la toma de decisiones.

b) Establece la necesidad de un *plan informático estratégico de tecnología* que debe estar alineado a los planes institucionales, esto con el fin de unir esfuerzos en pro de una meta. Los planes manejados deben estar desagregados a un nivel tal, que permitan conocer, entender, controlar y direccionar las actividades; pero antes de su ejecución se requiere la debida aprobación y su posterior supervisión de manera periódica.

c) Las *políticas y procedimientos* se orientan a buscar el orden dentro de la entidad, definiéndolas tanto para el personal de TI como para los respectivos bienes tangibles o intangibles relacionados. Se determina la necesidad de distinguir: responsables, supervisión, sanciones, etc.; pero como punto clave

se distingue el ser dadas a conocer, lo cual se puede traducir en la generación e implementación de un Plan de Comunicación.

Cabe resaltar que la normativa establece la necesidad de *incorporar controles, sistemas de aseguramiento de la calidad y de gestión de riesgos, al igual que directrices y estándares tecnológicos*. (Contraloría General del Estado, 2009)

d) Los *proyectos tecnológicos* deben ser planteados de manera tal que se distingan claramente: aspectos de naturaleza, objetivos y alcance; los periodos planeados para su realización, costos bajos, el concepto de *costo total de propiedad (CTP),* responsables, ciclo de vida, ciclo de cambios y la evaluación de riesgos (Principalmente).

e) Respecto al *desarrollo y adquisición de software aplicativo* se menciona como elemento básico el manejo de un ciclo de proyectos así como la adopción de estándares internacionales para aspectos relacionados a la tecnología. Entre otros aspectos se habla de manejar especificaciones o requerimientos técnicos y funcionales, de cualquier proyecto que hayan sido debidamente aprobado esto con el fin de clarificar y permitir el desarrollo exitoso de las soluciones.

f) Respecto de las *adquisiciones de infraestructura tecnológica,* estas deben orientarse a servir a los propósitos institucionales. Se debe manejar un plan para dichas adquisiciones donde se visualicen aspectos relacionados a: riesgos, costos y beneficios considerando además un elemento primordial como el tiempo.

g) En relación al *mantenimiento y control de la información tecnológica* se destaca aspectos como la importancia de la actualización de los manuales, el manejo de un plan de mantenimiento tanto preventivo como correctivo para eventos que comprometan la infraestructura del área de TI y controles aplicados a los bienes así como otros aspectos complementarios.

h) En el ámbito de la *seguridad de la información* se considera aspectos primordiales como: la ubicación de los equipos de TI, el manejo de respaldos diferenciando el tipo de información, seguridad en el software y hardware, controles o mecanismos que permitan monitorear determinados eventos entre otros.

i) Se determina la necesidad de definir y manejar un *plan de contingencias* teniendo en cuenta que se debe establecer un plan de respuesta al riesgo, un plan de continuidad así como un ciclo de cambios; todo ello debidamente documentado y comunicado para que de esta forma sean cumplidos eficientemente.

j) Para la *administración de soporte de tecnología de información* se plantean revisiones de forma periódica y controles para: entrada, procesamiento y salida de información y todas las actividades o acciones relacionadas.

k) El *monitoreo y evaluación de los procesos y servicios* se debe llevar a cabo de manera periódica a través de la aplicación de indicadores y manejo de informes sobre los resultados. Esto con el objetivo de determinar *la contribución e impacto del uso de tecnología de información en la entidad.* (Contraloría General del Estado, 2009)

Los aspectos de la normativa enumerados anteriormente, se consideran claves para la entidad e inclusive aportan al cumplimiento de sus objetivos institucionales. Estos son usados posteriormente en la aplicación de *COBIT 5 para riesgos* en un proceso que permite llegar a la definición de las actividades que conformarán el plan de respuesta al riesgo de la DTIC basado en la aplicación de prácticas claves propuestas en *COBIT 5 procesos catalizadores.*

Como se mencionó en párrafos anteriores la normativa se basa en el modelo del marco COSO por ello, para recordar dicho marco en las siguientes líneas se rescatan conceptos y ejemplo de este.

2.4. COSO

El COSO (Committee of Sponsoring Organization) es un marco integrador que se puede aplicar dentro de cualquier organización indistintamente de sus características, ya que le brinda la opción de obtener mejores resultados relacionando los procesos, personas y estructuras, logrando así un mejor desempeño de la entidad y una adecuada supervisión de sus actividades.

Su creación fue un esfuerzo conjunto de varias organizaciones como: la Asociación de Contadores Públicos Norteamericanos (AAA), el Instituto Norteamericano de Contadores Públicos Certificados (AICPA), la Asociación Internacional de Ejecutivos de Finanzas (FEI), el Instituto de Gerentes de Contabilidad (IMA) y el Instituto de Auditores Internos (IIA) así como personas o instituciones privadas. (PwC, 2013)

La importancia de aplicar un modelo que encamine el control interno de una entidad y a la vez permita definir la efectividad del mismo, convirtió al COSO en una herramienta adoptada por la dirección o gerencia de miles de empresas a nivel mundial. Su primera versión fue publicada en el año de 1992 Marco Integrado de Control Interno y hasta la fecha se ha publicado una versión mejorada que sustituye a la anterior, esta versión fue aprobada en mayo del 2013 bajo la denominación de Marco COSO 2013 y fue de total aplicación al 15 de Diciembre del 2014.

2.4.1. Control Interno

El concepto manejado en la versión anterior de COSO no ha sufrido cambios, se define entonces al control interno como: "*un proceso efectuado por la Junta Directiva, la gerencia y otro personal de la organización, diseñado para proveer seguridad razonable en relación con el cumplimiento de los objetivos en las siguientes categorías:*

- *Efectividad y eficiencia de las operaciones*
- *Confiabilidad de reportes*
- *Cumplimiento con leyes y regulaciones aplicables."* (Deloitte; Valero, Nelson; Roa, Mauricio;, 2013)

El objetivo primordial para una entidad es lograr los objetivos empresariales que han sido inicialmente establecidos. Para su definición previa se debía tener en consideración el objetivo de los socios, a raíz del cual inician un proyecto con miras a obtener ganancias (u otro dependiendo del tipo de entidad), pero unido a ello se manejan objetivos de competitividad, permanencia, reconocimiento por la calidad del producto y el entorno laboral, entre otros.

Indistintamente del objetivo, se vuelve necesario tener en cuenta varios eventos que pueden afectar tanto positiva como negativamente a los resultados. Dichos eventos se pueden relacionar con elementos tales como:

1. Mejores prácticas: aplicación, adaptación.
2. Personal: capacitación, ética y valores, ánimo, definición de roles y responsabilidades, etc.
3. Estructura organizacional
4. Infraestructura de la organización: edificios, maquinaria, TI, etc.
5. Leyes: entorno cambiante, situaciones políticas.

La aplicación de *mejores prácticas* le permite a la entidad la realización de sus objetivos de manera más eficiente, ordenada y responder oportunamente a las condiciones cambiantes del medio en el cual opera. Sin embargo, al existir una amplia gama de estas a veces la dirección puede no elegir la apropiada acorde a la naturaleza de la empresa o simplemente evitar su uso.

Aplicar un modelo no apropiado implica establecer controles, medidas y objetivos no realizables que llevan a la frustración de los administrativos; además provoca una pérdida de confianza por parte de las personas internas y externas involucradas con la información derivada del mismo y de las actividades realizadas.

El *personal* se considera clave para el desarrollo de cualquier actividad dentro de una entidad, su capacitación y competencia suficiente aporta a la entidad no solo con su trabajo sino proponiendo ideas o soluciones novedosas, llegando a sentirse parte de la misma.

Pero, este ambiente óptimo deseable depende en gran parte de los procesos adoptados previamente por la dirección o gerencia al momento de establecer controles y procedimientos para seleccionar-contratar personal y asegurar que las acciones permitan generar valor agregado.

Para que el personal pueda realizar sus actividades, se debe haber definido una *estructura organizacional* en la cual se encuentren perfectamente delimitadas: actividades, responsabilidades, autoridad y procesos internos a través de manuales, políticas por área, departamento, puesto de trabajo, etc.

Estas actividades se direccionan a lograr una óptima gestión operativa, que se relaciona a la eficiencia y eficacia de las actividades y se convierte en uno de los tres objetivos a los cuales el control interno brinda seguridad razonable. Sin embargo, un elemento indispensable se vuelve el control de los activos que maneja la entidad, es decir, *la infraestructura*. Una entidad debe supervisar y controlar el uso de cada uno de sus activos, protegerlos de daños internos y externos sean estos casuales o premeditados.

El daño, mal uso o pérdida de un activo le puede significar a la entidad pérdidas monetarias o de productividad e inclusive competitividad; por ello el instituir controles para estos bienes es indispensable.

La información se genera en todo proceso, ya sea interno o externo, que realice la entidad y su existencia constituye un activo intangible que se debe controlar. Las personas al interactuar generan información, al ingresar datos de sus actividades diarias en la base de datos también lo hacen.

Sin embargo, mucha de la información puede volverse repetitiva o irrelevante en la toma de decisiones por lo que debe necesariamente contar con una

seguridad razonable, también puede ser objeto de interés por parte de personas ajenas a la entidad que buscan oportunidades para disponer de la misma.

Se puede mencionar varios casos en los cuales la información está en peligro desde los siguientes enfoques:

a) INTERNO

La información como materia prima para tomar decisiones se deben establecer medios adecuados para su obtención y manejo. Tener un excelente sistema de información no garantiza la calidad de la misma, si el personal no conoce cómo manejarlo o si no se manejan ciertos parámetros de seguridad para acceso o modificación de la información.

La confiabilidad de la información se relaciona con la aplicación de controles en áreas críticas de la entidad, no es apropiado establecer controles en toda actividad que se realice ya que esto implica: costos, tiempo y al final la revisión de la información se vuelve tediosa, poco sustancial e inoportuna.

Respecto al personal, se debe prestar atención cuando se definen los términos de la relación laboral, en especial, cuando son cargos que manejan información clave del negocio por ejemplo: un empleado del área de TI, un administrador, un jefe departamental. Los controles se pueden referir a: cambio de contraseñas, eliminar usuarios, informar a toda la entidad sobre el cese de labores de un empleado, devolución de los accesorios o herramientas de trabajo así como llaves incluidas las copias de las mismas.

b) EXTERNO

En este ámbito se puede mencionar el ataque de *hackers* o el *concepto de reingeniería* social, que puede ser aplicado por personas ajenas a la entidad sobre los empleados de la misma buscando obtener una determinada información. Los controles empleados para este escenario incluyen: rotación de personal y la segregación del manejo de información, es decir, que no solo un empleado tenga acceso a la totalidad de información.

Como se evidencia la información es susceptible de daños y modificaciones motivadas o accidentales, que afectan directamente a la generación de información y en lo posterior a la toma de decisiones. La implementación de controles da mayor seguridad y confianza a las personas que dependen de la información aunque requiere de un análisis preliminar para su definición.

Finalmente, una entidad no está aislada, debe tener presente que se encuentra sujeta a disposiciones legales del país o países en los cuales realiza sus actividades. Por ello, la importancia de generar información confiable que sea útil para la entidad y a su vez permita el *cumplimiento* de disposiciones emitidas por los organismos reguladores.

2.4.2. Componentes del CI

El modelo COSO considera 5 componentes de la entidad, en los cuales es necesaria la implementación de controles para lograr la consecución de los objetivos institucionales. Dentro de estos tenemos:

- Entorno/Ambiente de control
- Evaluación de Riesgos
- Actividades de Control
- Información y Comunicación
- Actividades de Supervisión

El *entorno de control* constituye el componente base sobre el cual funcionarán los otros cuatro componentes, se refiere a establecer un ambiente idóneo donde las personas se puedan desenvolver diariamente. En este nivel se definen varios subcomponentes como son:

1) *Integridad y ética*: Se requiere que las personas que intervienen en las operaciones de la entidad manejen un determinado grado de valores al realizar sus actividades, es decir, se establece una conducta esperada para ellos. El personal debe ser seleccionado conforme a los valores corporativos.

2) *Competencia profesional:* Para que la organización logre un grado de productividad adecuado, las personas deben estar haciendo lo que mejor saben hacer, es decir cada puesto de trabajo se debe fijar acorde a la experiencia, habilidad y destreza del empleado de este modo se evita pérdida de tiempo y dinero así como la subutilización de recursos que son a menudo escasos.

3) *Filosofía y estilo de la organización:* Se refiere a la manera como se toman decisiones, se realizan las actividades y se fijan objetivos en la organización. Se pregunta ¿qué estilo operativo aplica la dirección? En la entidad se pueden presentar tres tipos de estilos: *autocrático, participativo y laisser-faire*; el primero, se caracteriza por la toma de decisiones impositivas en la cuales el personal, jefes de unidad y demás no tiene la opción de presentar sus ideas y proponer soluciones.

   El segundo, hace referencia a que en la entidad, todos o por lo menos un porcentaje considerable de las personas aportan con ideas y están comprometidas con el logro de los objetivos. Por último, el estilo laisser-faire implica que solo se deja que las cosas sigan su curso normal y se cumplan los objetivos, este es muy adaptativo. Ninguno de los estilos puede clasificarse como bueno o malo, todo dependerá de la empresa y su forma de adopción.

4) *Estructura Organizacional:* Constituye el marco en el cual se planean, ejecutan y controlan las actividades para el logro de los objetivos. Se evalúan aspectos referentes a como están distribuidas las áreas de trabajo según similitudes o conexiones (departamentalización), las actividades a realizar por persona y en la unidad o departamento (soportadas en la cadena de valor en la cual se definen actividades primarias y de apoyo), la coherencia y aplicabilidad del organigrama.

5) *Asignación de autoridad y responsabilidad:* La autoridad constituye un elemento de cohesión para la organización. Se vuelve de importancia la fijación de la responsabilidad para que los individuos puedan tener

iniciativas y trabajen conjuntamente dentro del límite de su autoridad. Estos dos elementos van de la mano con la relevación de información, por lo que se necesita la definición de canales de comunicación del tipo: unidireccional, bidireccional o multidireccional.

6) *Políticas y prácticas aplicadas al Talento Humano:* Como se mencionó en párrafos anteriores las personas constituyen un elemento, por ello se necesita la aplicación de controles en temas relacionados a: la contratación, capacitación y desarrollo, evaluaciones y remuneraciones. La definición de los controles debe encajar con leyes emitidas por organismos de control y demás que tengan relación al personal. Como referentes de leyes tenemos: Código de trabajo, LOES y su reglamento entre otras.

7) *Directorio y Comité de Auditoría:* Conjunto de dos o más personas internas o externas a la entidad que se encargan de proveer orientación, establecer autoridad, la vigilancia y supervisión. En general se encarga de establecer criterios para el ambiente de control.

La *evaluación de riesgos* se considera un proceso dinámico, en el que varias personas interactúan para definir los riesgos tanto internos como externos a los cuales se expone la entidad y puede afectar la consecución de sus objetivos ya sean estos de operación, información o de cumplimiento.

Para poder establecer con claridad y objetividad dichos riesgos es necesario que las personas conozcan de manera integral la empresa, estos es, que identifiquen con facilidad puntos débiles y fuertes de la organización. Como guía en este conocimiento se emplea las tres categorías de objetivos básicos en una entidad.

Una vez identificados los puntos débiles de la entidad se procede al análisis de los motivos o circunstancias que provocan estas fallas, para esto se necesita información proveniente de varias unidades de la organización. En base de dicho

análisis se puede proceder a la evaluación del riesgo considerando dos aspectos: impacto y probabilidad del mismo.

Por ***impacto*** se debe comprender como las consecuencias o efectos que se presentarían en la entidad si el riesgo se materializa. El impacto podrá ser clasificado como: alto, medio o bajo según las consecuencias sean graves, considerables o pequeñas, respectivamente. Por otro lado, la ***probabilidad*** es la posibilidad subjetiva u objetiva de que el riesgo se llegue a materializar esto dependerá del tipo de información que se emplee para definir la probabilidad.

Si la entidad cuenta con información de experiencias pasadas en las cuales los riesgos fueron similares o incluso consigue información externa y ésta además es cuantitativa, entonces el porcentaje de probabilidad será más certero y cercano a la realidad. Sin embargo, si la entidad no cuenta con experiencias pasadas y la poca información que dispone es cualitativa entonces el porcentaje de probabilidad que se asigne a un riesgo será poco certera y dependerá de la intuición de quién esté a cargo.

La evaluación no solo se hará a los riesgos sino a la gestión de cambio por parte de la entidad. Esto significa, evaluar el escenario que se puede presentar en la organización respecto a los controles después de realizar ciertos cambios.

El componente *actividades de control* hace referencia a un agregado de políticas, procedimientos y acciones llevadas a cabo por las personas bajo el mando de la dirección cuyo objetivo es asegurar el cumplimiento de los sistemas existentes en la organización. Una empresa puede manejar varios sistemas internamente como: de tecnologías de información y comunicación, de motivación entre otros; dentro de los cuales se encuentran establecidas tareas, actividades, procesos a realizar dentro de su puesto de trabajo.

Este componente implica la mitigación de riesgos. Las actividades podrán ser tanto manuales o automatizadas dependiendo del caso, por ejemplo: se pueden emplear procedimientos para el procesamiento de información o en general al

sistema de información, y fijar controles para asegurar que dichos procedimientos son confiables y la información es correcta.

- ✓ Ejemplo 1: Si un cliente desea realizar un pedido en la empresa y además quiere acceder a un crédito, entonces el encargado del área de ventas primero revisará la BD para confirmar que es cliente y posteriormente le indicará que es necesaria una recomendación de un proveedor. (Procesamiento)

- ✓ Ejemplo 2: Revisión del tráfico de información en las redes y actualización de la configuración de los cortafuegos. (Sistema)

Ninguna actividad es cien por ciento efectiva pues de una u otra forma, un determinado control puede ser obviado intencionalmente o por error humano, por ello los controles se deben instaurar con el fin de: detectar, prevenir o corregir un hecho.

Dentro del componente de *información y comunicación* se debe tener presente que "*la información es necesaria para que la organización pueda llevar a cabo sus responsabilidades de control interno y soportar el logro de los objetivos"*. (PwC, 2013)

La comunicación y la información son diferentes conceptualmente en su significado, pues la primera hace referencia a la interacción de las personas y a difundir un mensaje pero este puede o no ser información, esto dependerá si incrementa o no el conocimiento del receptor. Además la información es un proceso unidireccional mientras que la comunicación es bidireccional.

Los sistemas existentes producen información que es usada para la toma de decisiones o se convierten en materia prima para otros sistemas. La comunicación dentro de la institución puede ser *formal o informal* dependiendo de los medios utilizados y de la afinidad con respeto a la jerarquía. Es importante definir los canales de comunicación de manera que se logre eficiencia y darlos a conocer a todos en la entidad para que puedan saber cómo realizar un pedido, sugerencia, aporte de ideas entre otros.

Ejemplo: Dentro de los sistemas de información se puede mencionar un sistema contable así como manejo de documentos comerciales (recepción, registro, archivo y demás), mientras que un sistema de comunicación se puede identificar claramente en las charlas establecidas diariamente en el área de trabajo y existe retroalimentación.

Finalmente, el quinto componente hace referencia a las *actividades de supervisión* también conocido como supervisión y monitoreo. Conocer e informarse de todo lo que sucede dentro de la entidad así como las relaciones con partes externas es necesario, de esta manera se evitan problemas de eficiencia y eficacia en el logro de objetivos esto incluye conocer si los controles definidos para los componentes anteriores están siendo aplicados y si se acoplan a la realidad de la entidad o necesitan ciertos cambios.

El tipo de supervisión a aplicar dependerá de la importancia del proceso o actividad a vigilar, podrá instituirse una supervisión *continua* que vendrá por defecto vinculado a un sistema, ejemplo de ello constituye la dirección de TIC, en la cual se debe supervisar continuamente los contratos de outsourcing para determinar el rendimiento y cumplimiento de requerimientos.

También se puede aplicar una supervisión *separada* por ejemplo a un activo fijo y su aseguramiento que se realiza cada determinado periodo de tiempo.

CAPÍTULO III

MEJORES PRÁCTICAS

Este capítulo tratará tres marcos estándar relacionados a la Gestión de Riesgos y Seguridad de la información, concluyendo con una comparación de estos para establecer un bosquejo que ayude a tomar una decisión final direccionada a implementar COBIT 5 *para Riesgos.*

Las normas a tratar son:

1) ISO 31000: Gestión de Riesgos – Principios y Directrices
2) ISO 27005: Gestión del Riesgo en la Seguridad de la Información 3) COBIT 5 para Riesgos

Daisy Fernanda Alvarado Carpio
Laura Alexandra Zumba Morales

3. MEJORES PRÁCTICAS

3.1. Antecedentes

Actualmente toda entidad independientemente del medio en el cual se desenvuelva, experimenta una creciente exposición a los riesgos, ya que conforme avanza la globalización su dependencia a los sistemas de información se hace más evidente, puesto que la tecnología informática constituye una base para el desarrollo de cada proceso dentro o fuera de la entidad. Su *control y admi*nistración no solamente se encuentra a cargo de la máxima dirección sino también se direcciona al personal en los diferentes niveles.

Al hablar de gestión de riesgos debemos entenderla como un proceso dinámico, el cual engloba la aplicación de varias acciones que debidamente estructuradas y aplicadas de forma integral permite a la organización identificar y evaluar los riesgos que impiden el cumplimiento de sus objetivo. La gestión no se limita a un evento o circunstancia lo cual permite la identificación de debilidades y amenazas a las que se encuentra expuesta toda la entidad pudiendo así ampliar y mejorar las decisiones al proporcionar respuestas integradas a los múltiples riesgos. (Mejía, 2006)

Su objetivo primordial es maximizar las oportunidades y minimizar las pérdidas, buscando un equilibrio entre riesgo y oportunidad, de acuerdo con la tolerancia al riesgo que ha definido la organización en la realización de sus operaciones.

La implementación de esta gestión permite a una entidad alcanzar una variedad de objetivos, entre ellos:

✓ Asegurar su supervivencia, garantizando la continuidad de las operaciones evitando así la interrupción de sus servicios y pérdidas financieras significativas, que pueden afectar su imagen o los planes de desarrollo.

✓ Emplear eficiente y eficazmente los recursos físicos y financieros así como el talento humano para que contribuyan al logro de los objetivos, incremento de

la productividad y se descarten: pérdidas, subutilización, sobrecostos y desperdicios.

✓ Mitigar pérdidas económicas relacionadas con la ocurrencia de los riesgos, mediante la disminución de la incertidumbre de las operaciones hasta aquellos límites establecidos como tolerables y también mediante la implementación de controles con el fin de evitar desviaciones en la consecución de los objetivos institucionales.

✓ Garantizar la disponibilidad y calidad de la información necesaria para la adecuada toma de decisiones y la administración de las operaciones así como aquella generada para terceros, de manera que ésta sea oportuna y eficiente.

✓ Lograr que las actividades de la empresa se realicen según las normas internas y externas vigentes a través de una vigilancia permanente.

✓ Generar y mantener una buena imagen ante el público general y los diferentes grupos de interés logrando en ellos confianza y credibilidad. (Mejía, 2006)

De ahí que la esencia de la gestión de riesgos radica en la implementación de acciones de tratamiento y control eficaces más que en una metodología muy detallada y compleja para la identificación, el análisis y la valoración; ya que esta gestión le da a la organización un carácter preventivo y proactivo, que contrasta con el carácter reactivo de aquellas prácticas administrativas que se centran en la solución cotidiana de problemas.

COBIT 5 para Riesgos se complementa con varios estándares internacionales relacionados con la Gestión de Riesgos, los cuales pueden ser implementados según las necesidades y capacidades de cada entidad. Para que estas normas tengan funcionalidad idónea deben ser evaluadas en aspectos: económicos, medioambientales, entre otros a fin de definir si aportan al cumplimiento de los objetivos de un gobierno corporativo.

3.2. ISO 31000: Gestión de Riesgos - Principios y Directrices

3.2.1. Antecedentes

ISO 31000 constituye un conjunto de normas relacionadas con la Gestión de Riesgos, puede ser utilizada por cualquier entidad: pública, privada, sin fines de lucro, asociaciones entre otras; ya que no se direcciona a una industria o sector en particular. Su objetivo es ayudar a la entidad a gestionar el riesgo con efectividad.

Esta norma suministra los principios, el marco de trabajo (framework) y un proceso destinado a gestionar cualquier tipo de riesgo en una manera transparente, sistemática y creíble dentro de cualquier alcance o contexto.

3.2.2. Principios

La norma establece una gama de principios que deben ser cumplidos por una entidad, en sus distintos niveles, para poseer una gestión eficaz del riesgo, estos se presentan a continuación:

La gestión de riesgos	Crea proyectos de valor
	Es parte integral de todos los procesos de la entidad
	Aborda explícitamente la incertidumbre
	Es sistemática, estructurada y oportuna
	Es adaptable
	Toma en cuenta factores humanos y culturales
	Es transparente e inclusiva
	Es dinámica, reiterada y sensible al cambio
	Facilita la mejora continua de la entidad
	Utiliza la mejor información disponible

Figura 9 Principios de la ISO 31000
Fuente**:** (International Organization for Standardization, 2009)

ISO 31000 también recomienda a las organizaciones que desarrollen, implementen y mejoren continuamente un marco de trabajo, esto con la finalidad

de lograr la integración del proceso de gestión de riesgos en el gobierno corporativo de la entidad, planificación y estrategia, gestión, procesos de información, políticas, valores y cultura.

3.2.3. Marco de referencia

Para que la gestión de riesgos tenga éxito requiere de la eficacia del marco de gestión de riesgo, este ayuda a lograr efectividad a través de la consideración de los riesgos en diferentes niveles y dentro de contextos específicos de una entidad. También colabora con la entidad al integrar la gestión de riesgos en su sistema de gestión global adaptando los componentes del marco a sus necesidades específicas. Si una entidad ha adoptado ya un proceso formal de gestión de riesgo este debe ser supervisado y evaluado de acuerdo a esta norma internacional.

A continuación se explica los pasos a seguir para el diseño de un adecuado marco de referencia:

Figura 10 Marco de Referencia ISO 31000
Fuente: (International Organization for Standardization, 2009)

Mandato y compromiso.- La introducción de la eficiencia en la gestión de riesgo requiere un compromiso firme y sostenido por la dirección de la entidad.

Diseño del marco para la gestión de riesgo.- Pretende de la evaluación y entendimiento tanto del contexto externo como interno de la entidad antes del diseño y aplicación del marco.

- *Establecimiento de la política de gestión de riesgos.-* En este se establece claramente los objetivos de la entidad para lograr un compromiso con el riesgo.

- *Responsabilidad.*- La entidad debe asegurarse de que haya rendición de cuentas, así como también la autoridad y las competencias adecuadas para gestionar el riesgo y garantizar la efectividad y eficiencia de los controles.

- *Integración de los procesos de la entidad.*- El proceso de gestión de riesgos debe ser parte de, y no separable de, los procesos de la entidad. El proceso debería incorporarse en la política de desarrollo, de negocios, de planificación estratégica, de revisión y gestión de procesos de cambio. La entidad con el fin de que se implemente la política de gestión de riesgos deberá poseer un plan de gestión de riesgos el mismo que puede ser integrado en otros planes de entidad, como un plan estratégico.

- *Recursos.*- Consiste en la asignación adecuada de los recursos por parte de la entidad para la gestión de riesgos.

- *Establecimiento de la comunicación interna y los mecanismos de información.*- Cuyo fin es apoyar y fomentar la rendición de cuentas y la propiedad de riesgo.

- *Establecimiento de la comunicación externa y los mecanismos de información.*- La entidad debe desarrollar e implementar un plan de cómo va a comunicarse con las partes interesadas externas.

Implementación de la gestión de riesgos: Para lo cual se tendrán en cuenta los siguientes aspectos:

- *Aplicación del marco para la gestión del riesgo*
- *Implementación del proceso de gestión de riesgos* (International Organization for Standardization, 2009)

Seguimiento y revisión del marco.- Mediante este la entidad podrá lograr una gestión de riesgo eficaz ya que a través de la medición del desempeño de su gestión en relación con indicadores, avances y desviaciones del plan de gestión de riesgo y la emisión del informe sobre el riesgo, podrá determinar que

la gestión de riesgo implementada sigue apoyando el desempeño organizacional.

Mejora continua del marco.- Las decisiones de mejora en la gestión de riesgos de la entidad y su cultura se tomarán en base a los resultados obtenidos del seguimiento y revisión del marco de las mismas, se sabrá decidir sobre cómo se puede mejorar la gestión de riesgos ya sea en el marco, la política o el plan.

3.2.4. Procesos

Se plantea una metodología que permite incorporar el riesgo dentro de la entidad, haciendo que este sea parte integral en programas o proyectos, departamentos y en general de toda la entidad conjuntamente con el apoyo y aporte de las partes interesadas.

El riesgo se encuentra presente de manera activa en la realización de las funciones y actividades del gobierno, así como en el ambiente interno de la entidad que se ha generado por las necesidades y naturaleza de la misma. El proceso de gestión de riesgo plantea cinco etapas.

3.2.4.1. Establecer un contexto

Referido al análisis y definición del ámbito en el cual se pueden presentar los riesgos y puntos claves que son necesarios al momento de diseñar la estructura para la gestión de dichos riesgos. Para ello, es necesario distinguir dos ámbitos que pueden afectar la consecución de los objetivos: interno y externo; el primero se enfoca en mantener un alineamiento entre cultura, procesos, estructuras y estrategias de la entidad con el proceso de gestión.

Mientras que el segundo se enfoca en definir y entender al ambiente que rodea a la entidad como: leyes, política, economía y demás que pueden ejercer cierto tipo de influencia o limitación a la hora de definir criterios de riesgo, así como la consecución de objetivos.

Una vez que se ha delimitado esta información, se genera el contexto para el proceso de gestión riesgos, mismo que además deberá contener datos sobre:

costos, recursos, responsabilidades y demás, de esta manera el proceso estará fundamentado y adaptado a la realidad de la entidad.

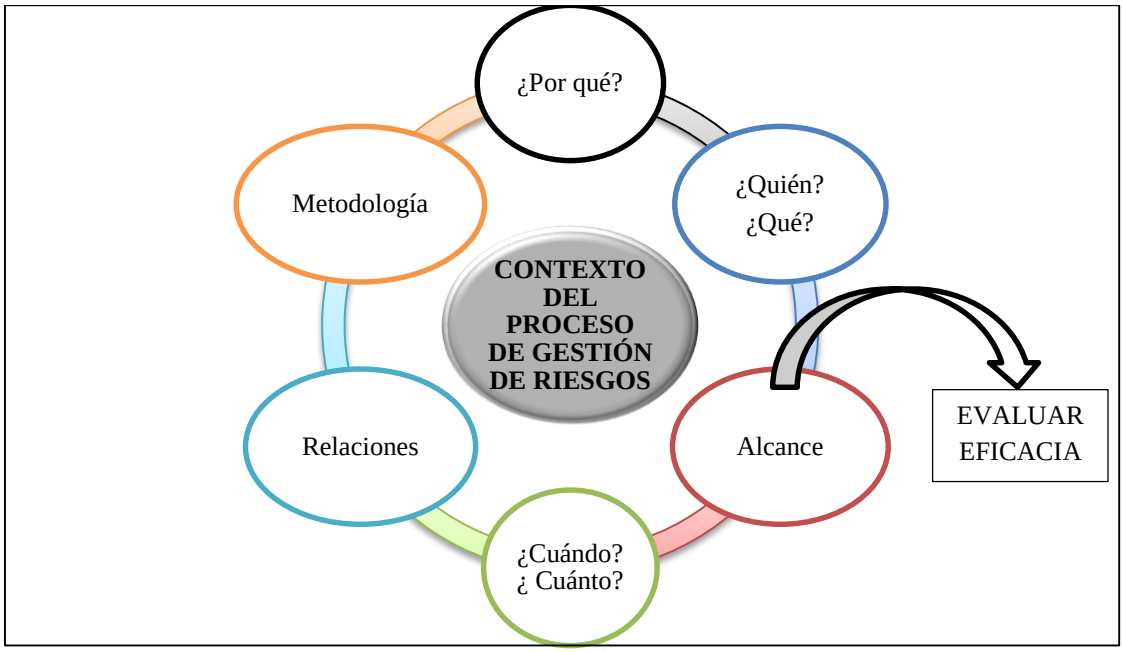


Figura 11 Resumen contexto del Proceso de Gestión de Riesgos con ISO 31000
Fuente: Autoras

La definición de los criterios de riesgos es substancial, ya que permite evaluar la significancia del riesgo, es decir, son parámetros que servirán para indicar la importancia del riesgo para la entidad; dichos parámetros pueden ser: naturaleza de la entidad, tipo de riesgo, probabilidades, tiempo, leyes, etc.

3.2.4.2. Valoración del Riesgo

Comprende puntos claves como la identificación, valoración y evaluación de riesgos que permiten conocer y tratar el ambiente de riesgo en el cual opera la entidad.

La *identificación* consiste en definir ya sea por áreas, departamentos, actividades o proyectos aquellos eventos que pueden ejercer influencia al momento de materializar los objetivos de la entidad.

Es vital la generación de un listado de dichos riesgos con especificaciones claras para cada uno, respecto a lo que podría ocasionar el evento (razón, motivo

o circunstancia) y cómo se vería afectada la entidad, considerando los efectos al corto y largo plazo.

Debido a la importancia de la actividad, se requiere de un personal adecuado para llevar a cabo su ejecución, debe cumplir con requisitos de: competencia, experiencia, destreza, entre otras; estas restricciones aseguran que no se omitan riesgos que pueden ser críticos, que al no ser detectados no se incluirán en análisis futuros afectando a la entidad.

El *análisis* implica entender el riesgo como tal. Para ello se profundiza en la información previamente obtenida, lo que implica definir factores que pueden desencadenar o favorecer la ocurrencia de un evento, los recursos necesarios y realmente disponibles para hacerle frente a la situación, etc. Dicho análisis puede ser: cualitativo, cuantitativo o mixto.

Se analiza además el impacto y probabilidad. La información constituye un pilar fundamental para evaluar el riesgo y la posterior toma de decisiones.

La *evaluación* parte de la priorización de los riesgos analizados, de esta manera la entidad puede enfocar su accionar de manera efectiva. Esta actividad consiste en comparar el criterio de riesgo definido inicialmente en el contexto versus el obtenido del análisis; el resultado obtenido permite elegir las medidas de tratamiento para corregir las desviaciones.

3.2.4.3. Tratamiento del Riesgo

Las opciones para tratar o responder al riesgo son varias y su elección depende de factores como: la naturaleza de la entidad, el presupuesto manejado, entre otros influyendo fuertemente el riesgo residual de las diferentes opciones.

OPCIONES: Evitar, incrementar, remover, compartir, retener, modificar el impacto o las probabilidades. → Combinación

Adicionalmente, para cada opción se debe considerar un análisis costo-beneficio y debe existir comunicación con las partes al respecto, ya que pueden

existir diferentes perspectivas respecto a una misma opción lo que conlleva a la necesidad de consensos.

Las decisiones tomadas se plasman en un Plan de Tratamiento del Riesgo que presenta los riesgos priorizados e información suficiente que cubre varios puntos claves que permite llevar a cabo su compresión e implementación.

En la elaboración de dicho plan se debe tener presente que en ciertas ocasiones una elección puede ayudar a cubrir ciertas deficiencias, pero también pueden generar nuevos riesgos que deben ser contemplados y presentados de la misma forma que los riesgos priorizados.

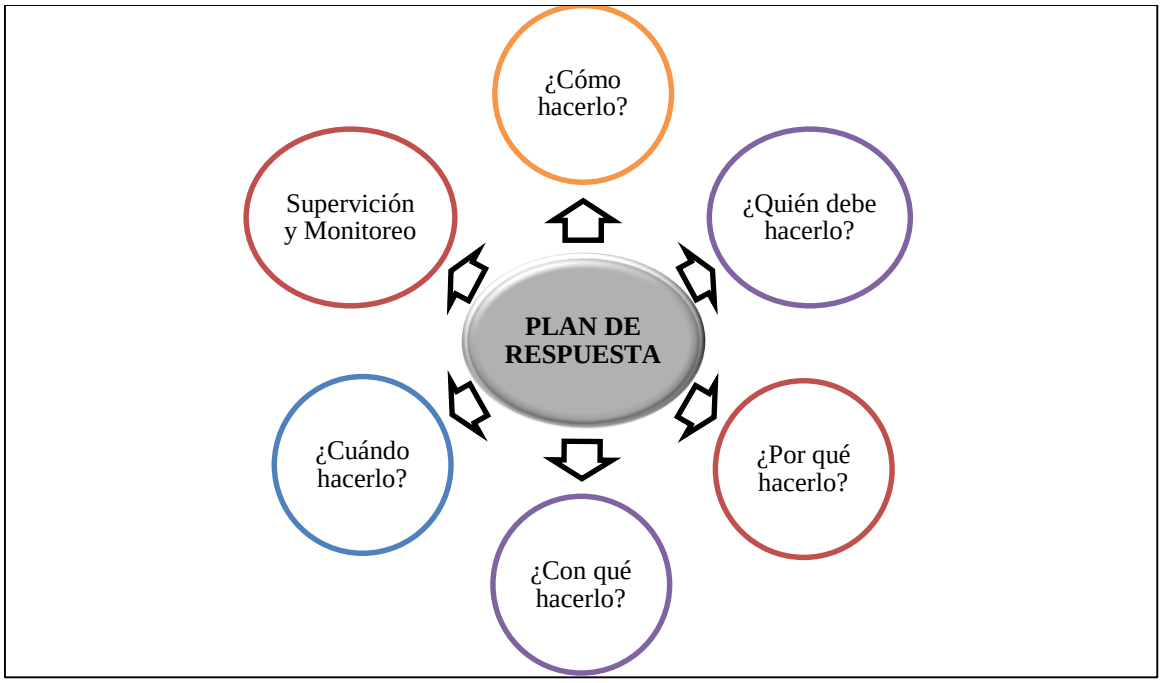


Figura 12 Elementos del Plan de Respuesta
Fuente: Autoras

3.2.4.4. Monitoreo y revisión

Estas dos actividades forman parte de la planeación de la gestión de riesgos, implican efectuar un chequeo de manera regular o una vigilancia oportuna de aquellas actividades o procesos que han sido objeto de correcciones, esto con el fin de brindar cobertura total a dicho proceso o identificar incluso nuevos riesgos que requieran de atención. La responsabilidad sobre dichas actividades debe ser previamente identificada y dada a conocer dentro de la entidad.

3.2.4.5. Comunicación y consulta

Ambas actividades deben ser aplicadas durante todo el proceso de la gestión de riesgos, por tanto para que tengan un adecuado funcionamiento y ayuden al cumplimiento de los objetivos, las formas y maneras de llevarlas a cabo deben ser plasmadas en un Plan de Comunicación que debe ser dado a conocer a lo largo de toda la entidad.

El objetivo principal que se persigue es asegurar que los encargados de la gestión de riesgos así como las partes interesadas estén al tanto de cómo son tomadas las decisiones y comprenden las actividades que se deben llevar a cabo dentro de la entidad.

La realización de las actividades además se direcciona a facilitar un proceso de intercambio de información veraz, relevante, preciso y que sea entendido por todos los integrantes.

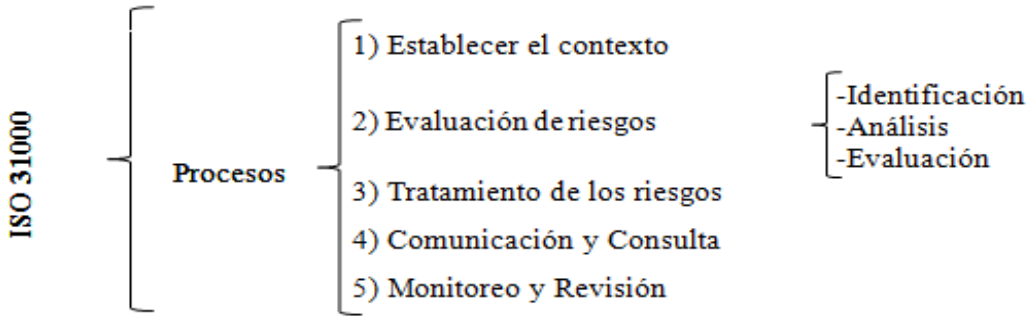


Figura 13 Resumen del Proceso de GR según ISO 31000
Fuente: (International Organization for Standardization, 2009)

3.3. ISO 27005: Gestión del Riesgo en la Seguridad de la Información

3.3.1. Antecedentes

La serie de las normas 27000 se enfocan en la Gestión de Riesgos para la Seguridad de la Información, desde diferentes perspectivas y enfoques, pudiendo cualquier entidad adoptar alguna de estas conforme sus necesidades. La familia 27000 se encuentra compuesta por las siguientes ISOs:

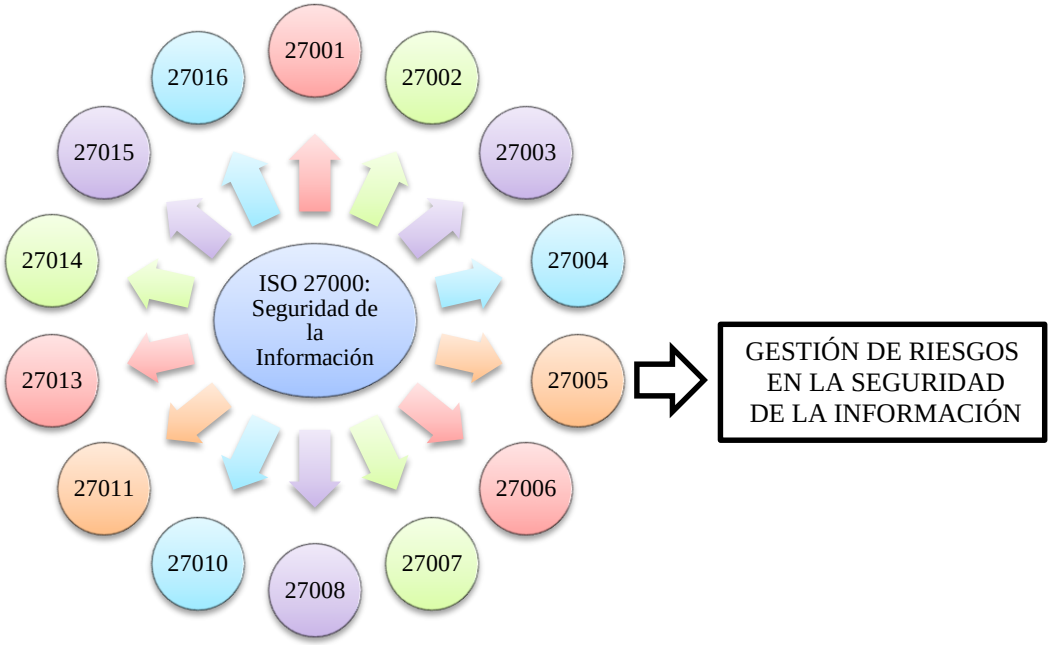


Figura 14 Familia ISO 27000
Fuente: (International Organization for Standardization, 2015)

La ISO 27005 es aplicable en todo tipo de entidad (de manera general o por partes), se direcciona a gestionar los riesgos que podrían afectar a la seguridad de la información y por ende a la consecución de los objetivos empresariales. La norma suministra directrices para una efectiva gestión de riesgos, sin embargo, no constituye una camisa de fuerza al aplicarla ya que se adapta a la realidad de cada entidad.

Se trata de un enfoque sistemático que debería ser aplicado continuamente para el tratamiento de riesgos generados en el ámbito operativo de la entidad. Mediante su aplicación la alta dirección podrá analizar eventos que podrían suceder y los efectos que tendrían en la entidad antes de decidir la medida a implementar con el fin de reducir o aceptar los riesgos, llegando a tomar una decisión informada.

3.3.2. Proceso de Gestión de Riesgos

Las actividades para el Proceso de Gestión de Riesgos se resume en:

3.3.2.1. Establecimiento del Contexto

Básicamente se trata de entender el ámbito tanto interno como externo en el cual la empresa actúa, de manera que constituya una base para el proceso de valoración de riesgos y su posterior tratamiento. Consiste en plantear: los criterios básicos, el alcance y los límites así como una estructura adecuada que permitan el análisis posterior.

Respecto de los *criterios básicos* se pueden distinguir tres tipos de criterios:

Evaluación de riesgo cuyo fin es determinar el riesgo en la Seguridad de Información y se utiliza para determinar prioridades en el tratamiento del riesgo. Los aspectos claves que deben ser incluidos son: criticidad de los activos, aporte que da el activo al proceso operativo de la entidad, importancia de las características de la información, perspectivas de las partes interesadas entre otros.

Impacto: Implica determinar los daños y costos que se relacionan a un determinada actividad o a la entidad en su totalidad por la materialización de los riesgos. Los aspectos claves a considerar son: importancia de los activos, brechas en la seguridad, operaciones que ya no aportan al desarrollo de la entidad, entre otros.

Aceptación del Riesgo: Su definición depende de las políticas, metas u objetivos que la entidad se ha propuesto conjuntamente con la participación de las partes interesadas. Se refiere a la relación que existe entre un riesgo que se estima y el beneficio para el negocio. Al establecer los límites de aceptación se pueden presentar excepciones que implican sobrepasar una barrera impuesta, la misma que se puede dar únicamente en circunstancias definidas. Estos criterios, en general se pueden definir a corto o largo plazo dependiendo de la expectativa de la dirección.

Alcance y límites: para una entidad definir el alcance del proceso de gestión de riesgo, le asegura que se incluyan los activos relevantes en la valoración, mientras que los límites permiten direccionar las acciones referentes de riesgos.

Ambos aspectos se ven influenciados por el ámbito interno así como el externo que rodea a la entidad.

Estructura: Para llevar a cabo la gestión de riesgos en necesaria una estructura adecuadamente alineada que permita desarrollar funciones y responsabilidades, por ello se debe tener en cuenta requisitos básicos como: la implementación en el uso de un sistema de riesgo en la seguridad de la información, definir partes interesadas así como roles y responsabilidades de las personas en la entidad además de definir rutas para la toma de decisiones, etc.

3.3.2.2. Valoración del Riesgo

Se considera necesario una vez entendido el negocio y ámbito de actuación de los riesgos identificar, describir y priorizar los riesgos versus los criterios de evaluación del mismo y también con los objetivos relevantes de la entidad. Esta actividad en general toma como base la información generada en el establecimiento del contexto para después aplicar dos o más veces un proceso de identificación de riesgos, constituyendo la primera una especie de preámbulo a manera general y la segunda un análisis a profundidad únicamente de los riesgos considerados o calificados como prioritarios.

La valoración del riesgo tiene dos actividades principales que conllevan a la ejecución de actividades secundarias, la actividad que mayor realce tiene corresponde a:

Análisis del Riesgo.- La primera fase consiste en la **identificación del riesgo** que permite conocer que puede ocurrir dentro o fuera de la entidad que le cause una pérdida, respondiendo para ello preguntas tales como: dónde, porqué, cuándo, cómo entre otras. Se deben identificar los activos de la entidad, sean estos de su propiedad o solo para su uso, generando un listado en donde se recogen aspectos relacionados al valor que tiene para la entidad, los responsables de su manejo, los propietarios, etc.

La cantidad de información recolectada influye directamente en la valoración del riesgo por lo tanto, *más es mejor* siempre que ésta sea relevante. En base al

listado de activos identificados se definen las amenazas y sus orígenes. Se debe tener en cuenta que las amenazas pueden afectar a más de un activo y los resultados de estas también podrán ser diferentes dependiendo del mismo. Para definir las amenazas se puede acudir a aquellas personas que están directamente relacionadas con los activos y que conocen o identifican situaciones o se puede basar en la experiencia de situaciones anteriores. Otra opción es acceder a catálogos externos de riesgos. Sin embargo se debe recordar que las amenazas no son constantes al contrario son cambiantes.

Los controles que se manejan en la entidad o que se encuentran en fase de implementación pueden influir en la gestión de riesgos, es por ello, que se necesita realizar un análisis e identificación de estos, con el fin de evitar la duplicación de esfuerzos, aportar a su adecuado funcionamiento y eficacia así como establecer la necesidad de implantar controles complementarios. Un control puede ser considerado como: ineficaz, insuficiente o injustificado en el caso de los dos últimos se podrían mejorar, complementar o eliminar pero si es considerado como ineficaz simplemente se debe eliminar.

Una amenaza puede explotar una vulnerabilidad ya sea de un activo o varios y con ello afectar a la entidad, pero solo una vulnerabilidad no causa daño y una amenaza sin relación con una vulnerabilidad no constituye un riesgo.

Una vez que se han definido activos, amenazas, controles y vulnerabilidades, se pueden definir las consecuencias o resultados de la materialización del riesgo. La actividad se enfoca en los daños a: la confiabilidad, disponibilidad e integridad, recordando que los efectos pueden ser tangibles o intangibles. Para la identificación de las consecuencias es necesario trabajar con escenarios de incidentes. Las consecuencias pueden ser temporales o permanentes que pueden generar daños al valor monetario o estratégico de la empresa

La segunda fase consiste en la **estimación del riesgo** en la cual se pueden aplicar diferentes metodologías dependiendo del detalle de la información sobre el grado de criticidad de los activos, la magnitud de las vulnerabilidades

conocidas y los incidentes que las mismas han causado en la entidad, pero en general se diferencian tres tipos de metodología: cuantitativa, cualitativa y mixta.

La metodología más utilizada en la práctica es la cualitativa, debido a que permite una indicación general del nivel de riesgo y revelación de los riesgos más importantes. En el caso de requerir un análisis más específico y objetivo se puede emplear el método cuantitativo. Además, se deberá considerar que emplear un análisis cualitativo es menos complejo y costoso.

A continuación se detallan las estimaciones:

a) CUALITATIVO.- Este análisis se aplica cuando: los datos numéricos o los recursos no son adecuados o simplemente se dispone de información cualitativa. Su realización es adecuada para tomar decisiones, ya que se identifican los riesgos que requieren un análisis más detallado mediante el uso de una escala de atributos calificativos para describir la magnitud de las consecuencias potenciales (alta, intermedia y baja) y la probabilidad de ocurrencia.

VENTAJA	DESVENTAJA
Facilidad de comprensión por parte de todo el personal pertinente.	Dependencia en la selección subjetiva de la escala.

Figura 15 Método Cualitativo - Ventajas y desventajas

Fuente: Autoras

b) CUANTITATIVO.- Utiliza datos históricos sobre incidentes provenientes de varias fuentes, la calidad del análisis dependerá de lo complejo y exactos que sean los mismos; a diferencia del análisis cualitativo utiliza una escala con valores numéricos tanto para las consecuencias como para la probabilidad, las mismas que podrán variar de acuerdo con el tipo de riesgo y el propósito para el cual se va utilizar la salida de la valoración del riesgo.

Se deberá considerar y comunicar de manera eficaz la incertidumbre y la variabilidad tanto de las consecuencias como de la probabilidad.

VENTAJA	DESVENTAJA
El uso de datos históricos permite la relación directamente con los objetivos de seguridad de la información y los intereses de la organización.	Se puede dar cuando no se dispone de datos basados en los hechos que se puedan auditar, creando así una ilusión del valor y la exactitud de la valoración del riesgo.

Figura 16 Método Cuantitativo - Ventajas y Desventajas

Fuente: Autoras

c) MIXTO.- Combinación del método cuantitativo y cualitativo.

Una vez elegido el método se procede a definir el impacto de los incidentes de la seguridad de la información, pero cabe recordar que cuanto mayor sea la información se facilitará el proceso de toma de decisiones. Para la valorización del impacto se consideran dos aspectos: el valor de reemplazo del activo así como las consecuencias generadas para la entidad de una pérdida o compromiso del activo.

Para complementar el impacto es necesario definir la probabilidad de ocurrencia, es decir, asignar un porcentaje de posibilidad de qué un escenario de incidente ocurra, en el caso de que se requiera mayor exactitud se podrán agrupar o dividir los activos en sus elementos para posteriormente relacionarlos con los escenarios.

Por último, de la combinación entre impacto y probabilidad se puede definir el nivel de estimación del riesgo, el mismo que puede ser expresado cualitativamente o cuantitativamente.

Evaluación de Riesgo.- Consiste en la comparación de los niveles de riesgos anteriormente definidos versus los criterios de la evaluación y aceptación del riesgo. Las decisiones se toman en base al nivel de aceptación del riesgo, impacto, probabilidad y confianza en lo llevado a cabo, en la etapa de análisis del riesgo.

En resumen *la valoración del riesgo determina el valor de los activos de información, identifica las amenazas y vulnerabilidades aplicables que existen,*

identifica los controles existentes y sus efectos en el riesgo identificado, determina las consecuencias potenciales y finalmente prioriza los riesgos derivados y los clasifica frente a los criterios de evaluación de riesgos determinados en el contexto establecido. (Instituto Colombiano de Normas Técnicas y Certificación, 2009)

3.3.2.3. Tratamiento del Riesgo

Se trata de la definición y selección de determinados controles que se enfoquen en reducir, retener, evitar y transferir los riesgos todo ello plasmado en un plan de tratamiento.

La opción u opciones son elegidas en base al resultado obtenido en la evaluación del riesgo así como en un análisis costo-beneficio, considerando que tanto los riesgos prioritarios como aquellos considerados raros, pero con alto impacto, deben ser tratados. Entre las opciones para tratar el riesgo se ubican las siguientes:

- REDUCIR→ Tomar medidas que permitan disminuir a un nivel aceptable el riesgo.
- RETENER→ Nivel de riesgo satisfactorio en cuanto a criterios de aceptación.
- EVITAR → Eliminar aquellas actividades o acciones que representan riesgo.
- TRANSFERIR→ Compartir los riesgos con otras partes para así manejarlo eficazmente.

Algunos controles pueden parecer que requieren ser eliminados pero en realidad se debe considerar que a veces esto puede resultar más costoso que su permanencia por lo tanto la opción de retener o transferir, según sea el caso, puede ser la más adecuada.

3.3.2.4. Aceptación del Riesgo

Una vez identificadas las consecuencias de las opciones para tratar el riesgo, se toma una decisión que debe ser aceptada de manera total en aspectos de: responsabilidad, costos, consecuencias y demás, esto debe aprobarse de manera apropiada y formal. Sin embargo, se pueden presentar determinadas observaciones que obliguen a revisar los criterios de aceptación inicialmente definidos por no haber considerado sucesos extraordinarios.

3.3.2.5. Comunicación del Riesgo

Toda la información que se genere durante el proceso de gestión de riesgo debe ser compartida o comunicada con las partes interesadas, esto es fundamental al momento de generar un acuerdo sobre las maneras de gestionar riesgos. La comunicación se vuelve bidireccional, recordando que la percepción de cada individuo es diferente respecto de las situaciones por lo que deben ser analizadas o tomadas en cuenta al momento de elegir o seleccionar una opción. Los fines que se persiguen con esta actividad son seguridad, información, soporte, conocimiento, coordinación, concienciación entre otras.

3.3.2.6. Monitoreo y supervisión del Riesgo

Por el hecho de que los riesgos no son estáticos, que cualquier amenaza, vulnerabilidad o probabilidad pueden afectar de un momento a otro a un activo, es necesario mantener una visión general de la perspectiva del riesgo mediante una revisión y monitoreo de los mismos.

Respecto de los cambios aprobados y considerados como importantes, se definirán como prioritarios de la revisión, lo cual tendrá lugar de manera regular considerando las opciones seleccionadas para el tratamiento del riesgo.

La continuidad del monitoreo así como la revisión, permitirán que el contexto, resultado de la evaluación de riesgo y su tratamiento sean efectuados de una manera óptima. Todas las mejoras acordadas deben ser notificadas a los

directivos con el propósito de evitar alguna supresión o subestimación del riesgo, así como algún cambio en sus elementos.

La entidad debería verificar con regularidad que los criterios utilizados para medir el riesgo y sus elementos aún son válidos y consistentes con los objetivos, las estrategias y las políticas del negocio, y que los cambios en el contexto del negocio se toman en consideración de manera adecuada durante el proceso de gestión del riesgo en la Seguridad de la Información. (Instituto Colombiano de Normas Técnicas y Certificación, 2009)

3.3.3. Proceso de Administración del Riesgo

A continuación se sintetiza el *proceso de administración del riesgo* que dispone esta norma: (Instituto Colombiano de Normas Técnicas y Certificación, 2009)

1. Identificar y clasificar los recursos de información o activos que necesitan protección.

Se requiere que la entidad identifique sus activos de manera detallada diferenciando dos clases de activos.

a) *Primarios*: dentro de estos están las actividades y procesos de negocio así como la información. Se entiende por activos primarios a los procesos y a la información central de la actividad en el alcance. También se pueden considerar otros activos primarios tales como: los procesos de la organización, que serán más convenientes para elaborar una política de seguridad de la información o un plan de continuidad del negocio.
b) *De soporte*: hardware, software, redes, personal, sitio y estructura organizacional.

2. Valorización de los activos

Para este paso se debe definir la *escala* que se va a utilizar y los *criterios* para la asignación de una ubicación particular en esa escala para cada uno.

El uso de una *escala* cualitativa o cuantitativa es un asunto de preferencia organizacional, siempre que la elección sea pertinente para los activos que se

valoran. Ambos tipos de valoración se pueden utilizar para el mismo activo. Los términos típicos utilizados para la valoración cualitativa de los activos incluyen palabras como: insignificante, muy bajo, bajo, medio, alto, muy alto y crítico. La selección y la gama de términos empleados dependen de factores específicos en la entidad.

Los *criterios* utilizados como base para asignar un valor a cada uno de los activos deberán ser redactados en términos que no sean confusos. Dentro de los posibles criterios empleados para determinar el valor de un activo están: su costo original, su costo de reposición o renovación, o su valor puede ser abstracto. Otra base para la valoración de los activos es el costo en que se incurre debido a la pérdida de confidencialidad, integridad y disponibilidad después de un evento suscitado.

3. Evaluar las amenazas y vulnerabilidades y la probabilidad de ocurrencia

Para la evaluación se considerará que las *amenazas* pueden ser: deliberadas, accidentales o ambientales (naturales) y pueden dar como resultado daño, pérdida de los servicios esenciales entre otras consecuencias, dentro de las amenazas que también tienen importancia son las humanas.

Por otra parte con el fin de determinar los escenarios pertinentes de incidente se procede a la evaluación de las *vulnerabilidades* en las diferentes actividades, procesos o activos. Dado que las amenazas y vulnerabilidades han sido evaluadas se procede a obtener la probabilidad de ocurrencia de una amenaza específica, que está afectada por los siguientes aspectos:

- ✓ Lo atractivo que sea el activo y recursos, o el impacto posible aplicable cuando se toma en consideración una amenaza humana deliberada.
- ✓ La facilidad de conversión en recompensa de la explotación una vulnerabilidad del activo, aplicable cuando se toma en consideración una amenaza humana deliberada.
- ✓ Las capacidades técnicas del agente amenazador, aplicable a amenazas humanas deliberadas.

- ✓ La susceptibilidad de la vulnerabilidad a la explotación, aplicable tanto a vulnerabilidades técnicas como no técnicas.

4. Combinación de elementos: Una vez que los elementos del riesgos han sido establecidos estos son combinados para formar una visión general de los riesgos.

5. Definición de controles.- Dado que los riesgos han sido identificados, los controles existentes pueden ser evaluados o nuevos controles se pueden diseñar para reducir las vulnerabilidades a un nivel aceptable de riesgo.

6. Riesgo Residual.- El nivel de riesgo remanente, una vez que los controles han sido aplicados, es llamado riesgo residual y puede ser usado por la gerencia para identificar áreas en las cuales más controles son requeridos para reducciones adicionales de riesgo.

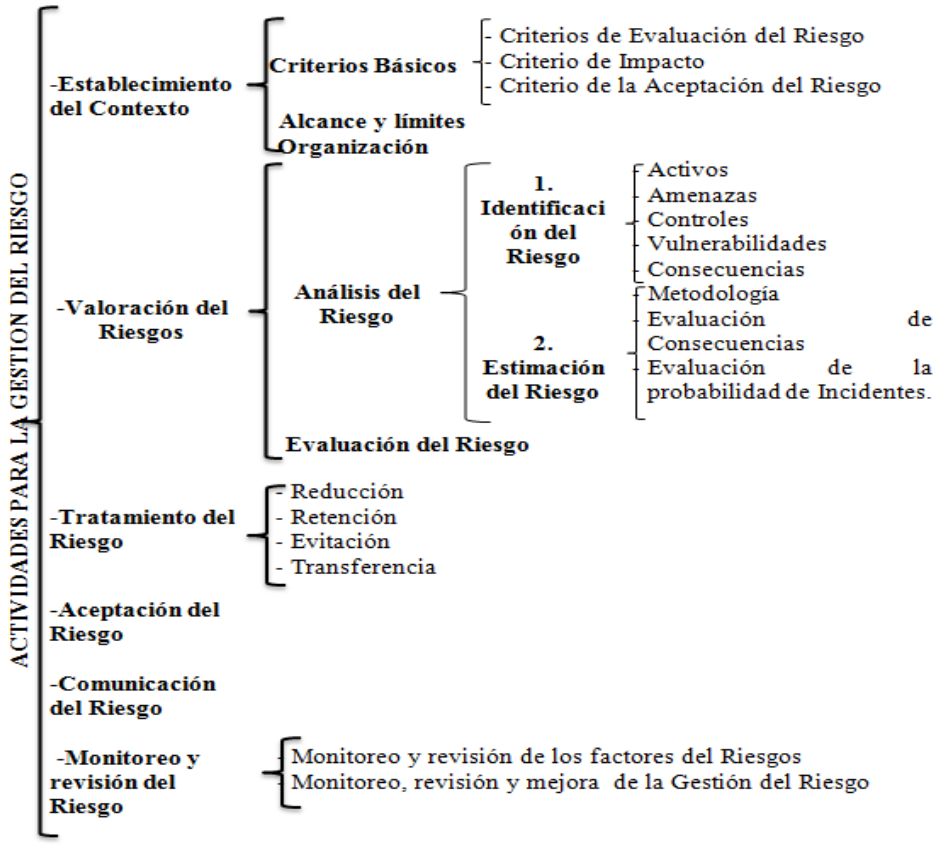


Figura 17 Resumen GR según ISO 27005
Fuente: (Instituto Colombiano de Normas Técnicas y Certificación, 2009)

3.4. COBIT 5

3.4.1. Antecedentes

La última actualización del marco de referencia fue el 10 de abril del 2012, fecha en la cual COBIT 5 integra todos los marcos anteriores Auditoría, Control y Gestión de Gobierno de TI llegando a ser hoy en día conocido como Gobierno Empresarial de TI el cual no se enfoca sólo en el área de TI, al contrario, actúa a lo largo de todas las actividades que contempla la entidad teniendo en cuenta a las partes interesadas.

COBIT 5 es un marco de referencia integrador versátil que puede ser aplicado a todo tipo de entidad, su fin principal es colaborar en el proceso de consecución de objetivos de la entidad, basado en la definición de una cascada de metas y la aplicación de siete catalizadores. Para alcanzar esto busca mantener el equilibrio

entre: las necesidades de las partes interesadas en relación a la generación de beneficios así como optimizar los recursos (monetarios, financieros, materiales entre otros) y los niveles de riesgo de la entidad.

No se trata de un lenguaje técnico de compleja aplicación, está más bien orientado a los negocios ya que busca que la entidad mantenga una total coherencia entre el Plan Estratégico Institucional y el Plan Estratégico de TI de manera que se dé la tan necesaria creación de valor para la entidad. Maneja un enfoque en el cual las TI se definen como parte importante del negocio, porque permiten desarrollar valor agregado para la entidad y generar así una ventaja competitiva.

Las entidades deben recordar que el marco no es una camisa de fuerza por tanto no constituye un modelo obligatorio, al contrario, lo que busca es que cada entidad tomando como base COBIT 5 estructure su propio *Gobierno Empresarial de TI.*

COBIT 5 se alinea con una variedad de estándares reconocidos y aceptados globalmente, como son: ISO 27000, COSO ERM, ISO 9001, ISO 31000, PMBOK (Project Management Body of Knowledge), CMMI (Capability Maturity Model Integration), etc., los cuales se usan como herramientas por auditores y administradores de negocios. COBIT 5 requiere ser complementado con varias herramientas ya que se encuentra mapeado con otros estándares.

COBIT 5 constituye toda una familia de productos relacionados a TI elaborados por ISACA, que es una asociación encargada de desarrollar metodologías y certificaciones que son aplicadas por miles de profesionales en el mundo en el ámbito de la auditoría y el control de los sistemas de información.

<table>
<tr><td colspan="5">COBIT 5 El Marco: Establece en marco general de trabajo: principios, catalizadores y aspectos para la definición de la cascada de metas (mapeo).</td></tr>
<tr><td colspan="5">GUÍAS DE CATALIZADORES</td></tr>
<tr><td colspan="2">COBIT 5 Información Catalizadora</td><td colspan="2">COBIT 5 Procesos Catalizadores</td><td>Otras guías de catalizadores</td></tr>
<tr><td colspan="5">Se enfocan es la descripción detallada de los catalizadores y su aplicabilidad.</td></tr>
<tr><td colspan="5">GUÍAS PROFESIONALES</td></tr>
<tr><td>Implementación de COBIT 5</td><td>COBIT 5 para Seguridad de la Información</td><td>COBIT 5 para Aseguramiento</td><td>COBIT 5 para Riesgos</td><td>Oras guías profesionales</td></tr>
<tr><td colspan="5">Brinda información de: cómo adoptar COBIT 5, mantener la seguridad de la información, actividades de aseguramiento y gestión riesgos.</td></tr>
<tr><td colspan="5">Entorno Colaborativo Online: Sitio web en el cual se encuentra soporte para uso de COBIT5 y da la oportunidad de interactuar con miembros de la entidad.</td></tr>
</table>

Figura 18 Familia de productos de COBIT 5
Fuente: (ISACA, 2012)

Según COBIT 5 en cuanto a la administración de riesgos se detalla lo siguiente: *"La gerencia en todos los niveles de la organización debería tener una adecuada comprensión del apetito del riesgo, requerimientos de cumplimiento y el impacto de los riesgos significativos de TI y otras operaciones en la gestión de riesgos que podrían impactar en forma individual o en toda la compañía en su conjunto. Por lo tanto, los altos ejecutivos deberían tener un claro entendimiento del apetito de riesgo que tiene la compañía, comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos, y la inclusión de las responsabilidades de riesgos dentro de la organización."*

COBIT 5 El Marco presenta una categoría del Riesgo de TI que considera tres tipos, estos son: (Valle, 2012)

1) **Riesgo de generación de valor de T.I. (ESTRATÉGICO)**.- Volver a enfocarse en los riesgos para consideraciones tales como cuan bien alineada esta la capacidad de las TI con las estrategias de negocio y su aprovechamiento con el fin de mejorar la eficiencia o efectividad de los procesos del negocio.

2) **Riesgo en la entrega de programas y proyectos de T.I (PROYECTO)**.- La administración de riesgos necesita enfocarse en la habilidad para

comprender y gestionar proyectos complejos de manera que no exista una deficiente contribución de las TI para las nuevas soluciones o mejoras.

3) **Riesgo en la entrega de servicios y operaciones de T.I. (OPERACIONAL)**.- Aquellos riesgos que podrían comprometer la efectividad de los servicios soportados por TI y la infraestructura de apoyo. Se debe recordar que el rendimiento y disponibilidad de los servicios de TI pueden influir directamente en el valor de la empresa llegando a reducirlo e inclusive destruirlo.

3.4.2. COBIT 5 para Riesgo

3.4.2.1. Bases de COBIT 5 para Riesgos

Este marco permite que se logre un mejor entendimiento sobre el impacto de los riesgos de TI a nivel de toda la institución, ya que es una guía de extremo a extremo para la forma de gestionar los mismos.

Para llevar a cabo la gestión de riesgo, COBIT 5 para Riesgos usa como base algunos aspectos importantes de COBIT 5 El Marco tales como: la diferenciación entre lo que es gestión y gobierno contenido en uno de sus principios, los catalizadores y la cascada de metas que son bases para identificar, analizar, responder y comunicar el riesgo a las partes interesadas de la entidad.

COBIT 5 se basa en cinco principios que son:

1. Satisfacer las necesidades de las partes interesadas → Crear valor
2. Cubrir la empresa de extremo a extremo → No solo TI
3. Aplicar un marco de referencia único e integrado → Alineación
4. Hacer posible un enfoque holístico → Interacción
5. Separar el gobiernos de la gestión → Diferenciación

La *gestión* se enfoca en cumplir las metas empresariales mediante el planteamiento, construcción, ejecución y monitoreo de las actividades cuya responsabilidad recae sobre la Dirección Ejecutiva bajo el mando del Director General Ejecutivo (CEO). Por el lado del *gobierno,* este pretende alcanzar las

metas corporativas enfocándose en las partes interesadas, es decir, evaluando sus necesidades, alternativas y realidades; su responsabilidad recae sobre el Comité de Entidad bajo el mando del Presidente.

La *cascada de metas* se basa en el análisis del contexto tanto interno como externo en el cual se encuentran inmersas las partes interesadas, pudiendo cualquier tipo de entidad optar por su utilización, ya que las necesidades de las terceras partes son expresadas en metas corporativas, aquellas relacionadas con TI y los catalizadores; las cuales sirven de apoyo para la consecución de los objetivos de la entidad de esta manera se garantiza una prestación de servicio óptimo.

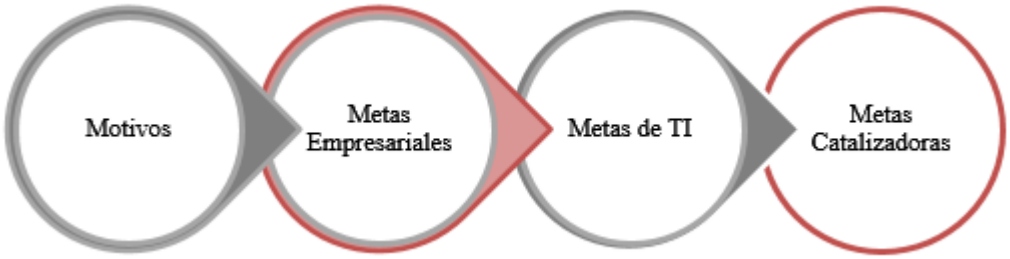


Figura 19 Cascada de Metas - COBIT 5
Fuente: (ISACA, 2012)

3.4.2.2. Perspectivas

COBIT 5 para Riesgos define dos perspectivas respecto al riesgo. La *primera perspectiva* es la función del riesgo que describe cómo construir y sostener la misma usando los catalizadores de COBIT 5, es decir, define una estructura modelo a ser aplicada en una entidad a fin de tener una adecuada organización que permita el control y administración de recursos, riesgos, beneficios, entre otros factores.

Un catalizador se define como una actividad que ayuda a determinar si algo funciona o no. El uso de los catalizadores ayuda a implementar y mejorar el gobierno, así como la gestión de TI en una entidad mediante un definido ciclo de vida, este consiste en: planificación, diseño, construcción, uso, evaluación y actualización. Los catalizadores son direccionados por la cascada de metas.

Los catalizadores usados para la consecución de las metas empresariales son:

1. Principios, políticas y marco de trabajo → Comportamiento deseado
2. Procesos → Entidad de prácticas y actividades
3. Estructura organizativa → Toma de decisiones
4. Cultura, ética y comportamiento → Factores de éxito
5. Información → Producto clave
6. Servicios, infraestructuras y aplicaciones → Procesamiento
7. Personas, habilidades y competencias → Actividades satisfactorias

La *segunda perspectiva* se enfoca en la gestión del riesgo, para lo cual se debe entender, definir e implementar como procesos centrales en la entidad EDM 03 así como APO12. Además se considera importante el uso de escenarios de riesgos pudiendo ser genéricos o levantados específicamente por la entidad usando como guía las prácticas de cada uno de los procesos de COBIT 5.

- EDM03 (Asegurar la optimización del riesgo): Asegura que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y luego gestionado.

- APO12 (Gestionar el riesgo): Permite identificar, evaluar y reducir los riesgos relacionados a las TI de forma continua, dentro de los niveles de tolerancia establecidos teniendo en cuenta los requerimientos de la dirección.

Para la segunda perspectiva se plantea la relación entre tres ítems claves para la gestión del riesgo estos son:

Proceso GR ↔ Escenarios de Riesgo ↔ Factores de Riesgo

3.4.2.3. Proceso APO 12: GESTIONAR EL RIESGO

I. Recopilar datos

La información y el conocimiento constituyen un elemento base para la realización de la gestión de riesgos, pues si el encargado de riesgos no conoce qué tiene a su cargo y qué debe gestionar entonces no podrá administrar.

Por ello, se considera necesario definir todo respecto a: procesos claves y secundarios, un método apropiado que permita recoger los datos para su posterior clasificación y análisis, datos relevantes sobre el ambiente en el cual se desenvuelve la entidad, información de eventos pasados que causaron problemas y en general datos históricos que sirvan de retroalimentación.

- **Descripción del ambiente actual:** Referido al entendimiento de información clave, que influye en la entidad y manejo del riesgo, tanto aspectos internos como externos comprendidos en: políticas, normas, procesos, leyes, regulación general, etc.

- **Priorización de procesos:** Para la priorización se utiliza el mapeo a través de la cascada de metas, tomando como base los objetivos corporativos para ser empatados con las metas genéricas que ofrece TI.

  Esto permite identificar las actividades que evitan la ocurrencia de riesgos según esta norma y direcciona las medidas de tratamiento.

II. Analizar el Riesgo

Uno de los objetivos del gobierno es optimizar el riesgo, lo que representa una parte esencial para la creación de valor, teniendo en cuenta que dicha optimización no se la puede separar de los demás objetivos, ya que todos se encuentran interrelacionados, es por ello, que el riesgo de TI requiere ser visualizado como un riesgo del negocio por tal motivo aspira a una óptima gestión riesgos, la cual le permita a la entidad reconocer y tener conciencia de cuáles son los riesgos potenciales a los cuales se enfrenta y contrarrestarlos o prevenirlos mediante el planteamiento de estrategias efectivas de gestión

evitando pérdidas o daños irreparables que imposibiliten el cumplimiento de los objetivos planteados.

Cabe mencionar que el ***riesgo*** es la probabilidad de que un evento ocurra y cause consecuencias (daños o pérdidas) que afecten la habilidad de alcanzar los objetivos, se mide a través de la probabilidad de que una amenaza se materialice explotando en una vulnerabilidad ocasionando así un impacto. Dentro de la entidad el riesgo siempre estará presente aun cuando no se lo haya reconocido o detectado.

Los riesgos típicos incluyen pérdida de productividad o negocios debido al tiempo de inactividad, responsabilidad por brechas de seguridad que exponen la información de los clientes, multas por violaciones de normas y la imposibilidad de defenderse de demandas debido a la conservación inadecuada de registros. No todos los riesgos provienen de sucesos inevitables, como una inundación o un terremoto, muchos de los riesgos informáticos son provocados por: contratiempos operacionales, procesos inadecuados, mayores requisitos normativos u otros factores controlables. (Chanocua, 2014)

Por otro lado, en el caso de siniestros una adecuada administración de riesgos nos permite la recuperación de las actividades de manera fácil, mediante la creación de planes de emergencia y contingencia que deberán ser elaborados y aprobados por las diversas áreas y procesos que pueden verse afectados por dichas situaciones. A continuación se presentan ejemplos de posibles amenazas, vulnerabilidades y riesgos que pueden presentarse en los sistemas informáticos

EJEMPLO CON COBIT 5		
AMENAZAS	**VULNERABILIDAD**	**RIESGOS**
Ingeniería social **Malicioso**	Falencias en capacitación del personal respecto a los nuevos métodos utilizados para una intrusión.	Información sensible sea revelada.
Inundación **Natural**	Ubicación incorrecta de servidores y ausencia de copias de respaldo para la información.	Destrucción de la infraestructura e información.
Falla	Ausencia de un plan de continuidad de aquellos procesos críticos para la entidad.	Interrupción de servicios
Accidental	Ineficiencia en los controles internos para el manejo de dispositivos.	Pérdida de un dispositivo portátil con información sensible

Figura 20 Ejemplo aplicados con COBIT 5 El Marco
Fuente: Autoras

El análisis de riesgos se relaciona con la definición de escenarios de riesgos de TI conforme la estructura de la entidad así como con los resultados de la información levantada, plasmando una calificación cualitativa y cuantitativa del nivel de riesgo. Para la calificación se deben clarificar conceptos relacionados, como:

- **Frecuencia.**- Número de veces que se repite un evento que afecta a la entidad.
- **Magnitud**.- Medida de las consecuencias que tiene un determinado evento para la entidad, ya sea de manera positiva o negativa.

Por lo antes mencionado, el nivel riesgo se expresa de manera cualitativa y cuantitativa de la siguiente forma:

N.R = Frecuencia * Magnitud

Estos términos, en otras prácticas para la Gestión de Riesgos se traducen en *probabilidad e impacto,* respectivamente. Los resultados cuantitativos obtenidos sobre el nivel de riesgo se traducen en una matriz que será empleada para dar a conocer a las partes el riesgo actual.

Matriz de Riesgo

Una matriz de riesgo pretende exponer una visualización aproximada y a la vez global de aquellos riesgos identificados que impactan a una entidad, permitiendo detectar y evaluar a simple vista si la gestión que ha se venido

desarrollando para el tratamiento de los mismos ya sean: operativos, estratégicos, proyectos; ha sido efectiva, es decir, se trata de una herramienta flexible que favorece a la adopción de medidas inmediatas considerando todas aquellas personas, áreas, unidades o departamentos que influyen activamente para que dichos riesgos sean contrarrestados de manera óptima.

Se puede apreciar los aspectos considerados como *críticos,* los cuales se encuentran sujetos a impactos negativos (daños, pérdidas), así como aquellos considerados como menos vulnerables. Sin embargo, todos tienen relevancia en la toma decisiones con el fin de reducirlos o superarlos y de esta manera lograr los objetivos institucionales o departamentales.

Esta matriz utiliza un grafo de riesgo, el cual se encuentra relacionada con la fórmula establecida para el *NR= Frecuencia * Magnitud.*

Las formas de presentar esta matriz son varias, dependiendo del criterio de la persona que se encargue de su elaboración así como los calificativos empleados para la descripción del estado del riesgo.

III. Mantener un Perfil de Riesgo

Se encuentra apoyado en el proceso EDM03: Asegurar la optimización del Riesgo, que permite la definición y comunicación de la tolerancia y apetito al riesgo que mantiene la entidad para sus actividades.

- **Tolerancia al Riesgo:** es el nivel aceptable de fluctuación del apetito de riesgo que inicialmente ha sido definido para el logro de los objetivos de la entidad.

- **Apetito al Riesgo:** es el riesgo que ha sido definido por los administrativos de la entidad como normal dentro de las operaciones de la misma, es decir, cuánto riesgo están dispuestos a aceptar como un medio para lograr los objetivos.

IV. Expresar el Riesgo

La comunicación oportuna del estado de los riesgos evaluados así como de las exposiciones a las cuales se encuentran sujetos los diferentes activos en la entidad, permitirá que tanto las personas internas y externas formen parte de respuestas pertinentes para tratar a los riesgos.

La comunicación del riesgo debe considerar la emisión de:

Plan de Comunicación de Riesgo.- En el cual se define la frecuencia, tipos y receptores de la información sobre el riesgo. Su propósito es prescindir de información irrelevante que imposibilite considerar los riesgos que requieren una atención oportuna. (ISACA, 2013)

Informe de los riesgos. Para dar a conocer los riesgos, se necesita manejar un documento formal que permita entender al receptor los resultados obtenidos ello se traduce en un *informe de riesgos*. Su fin es dar a conocer los riesgos detectados, independientemente de su nivel, y el perfil de estos mediante la especificación de atributos del Riesgo. (ISACA, 2013)

V. Definir un portafolio de acciones para la Gestión de Riesgos

Una vez definidos y dados a conocer los riesgos y sus atributos, se puede definir un portafolio que contenga propuestas para hacer frente a los riesgos, considerando en cada una de las opciones: el nivel de riesgo y las actividades clasificadas según criterios como: descripción, recursos de *COBIT 5*, responsables, métricas así como el riesgo residual entre otros ítems relevantes que se consideren necesarios para la toma de una decisión, siempre priorizando los riesgos, de manera que se atiendan los casos emergentes y que representan un mayor nivel de pérdida o impacto en la consecución de los objetivos.

Respecto al *riesgo residual*, su concepto se aborda posteriormente, pero en síntesis se trata del riesgo que tiene la entidad después de haber implementado las medidas para tratarlo. Para calcular su nivel se pueden optar por

ponderaciones, fórmulas pre-establecidas, reevaluación del impacto y probabilidad entre otras, dependiendo del criterio de la persona que lo aplica.

Adicionalmente, con los resultados obtenidos se puede realizar una serie de representaciones gráficas que ayuden a la comprensión e identificación de los riesgos de la entidad, antes y después de la gestión de riesgos.

Respecto de los *recursos COBIT 5* plantea cuatro categorías de estos:

1. Información: Hace referencia a los datos que resultan de la entrada, procesamiento y salida de los sistemas de información que una entidad utiliza en la realización de sus actividades y que sirven como materia prima, según su relevancia y oportunidad, para la toma de decisiones
2. Aplicaciones: Incluye los sistemas que son necesarios para el procesamiento de la información utilizados por los usuarios para automatizar las actividades que deben realizar, además de instrumentos adicionales como manuales y procesos requeridos para habilitarlos.
3. Infraestructura: Son aquellos sistemas, plataformas, hardware y demás herramientas tangibles o intangibles relacionados con la tecnología que le permite al usuario hacer uso de las aplicaciones.
4. Personas: Se entiende como aquellas que interactúan con la información y sus distintas herramientas, las cuales pueden ser internas o externas; se involucran en las decisiones de cuidado y elaboración de datos así como activos utilizados.

Para definir los *responsables* de llevar a cabo las acciones planteadas, se designan roles sobre:

- ¿Quién debe hacer?
- ¿Quién debe comunicar?

Finalmente, para que la acción pueda ser evaluada se considera necesario la formulación y posterior aplicación de *métricas* o indicadores que se relacionen con las actividades planteadas. Estos parámetros deben aplicarse periódicamente a fin de identificar la efectividad de los controles sobre los riesgos

así como la necesidad de cambios, si fueren necesarios, de una manera oportuna.

VI. Responder al Riesgo

Una vez analizado el riesgo conforme los niveles de apetito así como la tolerancia al mismo, y planteadas las actividades que se pueden aplicar para dar tratamiento, se debe establecer la respuesta que resultaría en caso de implementación.

Las respuestas al riesgo pueden ser las siguientes:

1. ***Evitar***.- Esta respuesta se adoptará cuando no exista otra opción adecuada que permita contrarrestar al riesgo, por tal motivo se optará por dejar de realizar las actividades o condiciones que dan lugar a que se desarrolle o materialice el riesgo.

2. ***Compartir/ transferir***.- Implica ceder los riesgo a las habilidades de otra parte en la gestión del riesgo con el fin de reducir las secuelas económicas o de otro tipo, en el caso de que llegue a darse un evento adverso consiguiendo así la reducción de la frecuencia o magnitud del riesgo. Frecuentemente, las prácticas empleadas para este tipo de respuesta son: seguros, outsourcing y la compartición de los riesgos con el proveedor a través de un régimen de precios fijos.

3. ***Aceptar.-*** Consiste en reconocer las pérdidas que puede ocasionar un riesgo pero aun así no se plantean medidas para tratarlo, las pérdidas aceptadas deberán ser comunicadas. Al optar por este riesgo se debe tener cuidado, es necesario establecer niveles de aceptación del riesgo lo cual ayudará a certificar que el riesgo es aceptado en el nivel correcto dentro de la entidad. En cuanto a los riesgos de TI deberán ser aceptados únicamente por la gestión empresarial con soporte en el área de TI.

4. ***Mitigar***.- Consiste en tomar medidas de atenuación para reducir la frecuencia o magnitud de un evento dañino, estas pueden ser: mejorar las

prácticas generales de gestión de riesgos de TI, implementar un número de controles de TI (políticas, procedimientos y prácticas, estructuras, flujos de información, etc.) o por otros medios o métodos (marco de gestión de riesgos de TI u otros estándares).

3.4.2.4. Escenarios de Riesgo

Inicialmente se debe diferenciar entre los tipos de riesgo:

1. Riesgo inherente: Es el riesgo existente en la entidad sin tomar en consideración ningún tipo de control o medida para su tratamiento.

2. Riesgo actual: Es el riesgo que la entidad tiene en un determinado periodo de tiempo (actualidad), una vez se hayan aplicado los controles. Se considera como el riesgo de hoy.

3. Riesgo residual: Constituye el riesgo actual una vez aplicadas las medidas de tratamiento para mitigarlo. Este siempre está presente ya que el nivel de riesgo nunca podrá llegar a cero independientemente de los controles o medidas tomadas.

Un escenario de riesgos se puede entender como la descripción detallada de los eventos o situaciones que pueden causar algún tipo de consecuencia positiva o negativa de alta, media o baja magnitud, en las actividades o procesos de la organización. Dichos eventos podrían afectar al: personal, procesos, objetivos y demás.

El desarrollo de escenarios de riesgo ayuda a la entidad a manejar de mejor manera sus actividades internas ya que le permite enfocarse en las situaciones con alto nivel de riesgo, permitiéndole vislumbrar su realidad. Para el desarrollo de dichos escenarios se debe tener en cuenta la aplicación de dos tipos de enfoques:

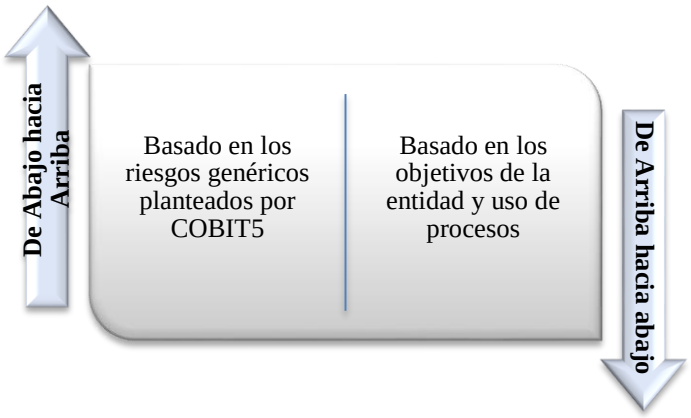


Figura 21 Perspectivas de los Escenarios de Riesgo
Fuente: (ISACA, 2013)

De Abajo hacia Arriba: Consiste en el uso de los escenarios presentados por el marco analizado, usando los mismos como una plantilla para el análisis posterior que permita reducir los riesgos.

De Arriba hacia Abajo: Consiste en definir los objetivos del negocio para posteriormente generar un listado de posibles eventos que afecten de manera importante a la consecución de los mismos.

Los dos enfoques se complementan entre sí y la entidad debe tener presente que es necesario adaptar la lista de escenarios genéricos a su situación particular.

COBIT 5 para Riesgos plantea una metodología denominada flujo de trabajo para escenarios de riesgos, se describen seis pasos para poder determinar un conjunto de riesgos que estén debidamente relacionados con la organización pero que a su vez sean filtrados de manera que el trabajo o las acciones correspondientes se enfoquen en situaciones de mayor peso por el grado de riesgo que estas representan.

Para el desarrollo del presente trabajo se han considerado agrupar algunos de los pasos, definiendo cuatro fases para determinar los diferentes escenarios de riesgos. Estos pasos se resumen en:

a) Escenarios Genéricos → Se trabajan únicamente con la lista de riesgos que se presenta en *COBIT 5*, y además se consideran los riesgos, a groso

modo, relacionados al ambiente externo que representen algún nivel de riesgo.

b) Comparación frente al negocio → Con la lista de escenarios genéricos se realiza una comparación con los objetivos de la institución así como del área de TI, las prácticas, los procesos y la lista de riesgos, de esta manera se pueden identificar aquellos riesgos que realmente obstaculizan la consecución de metas.

c) Universo manejable → Definidos los riesgos que afectan directamente a la consecución de objetivos se procede a priorizar los mismos, pues posteriormente estos serán objeto de tratamiento.

d) Detalle de los riesgos → Mostrar información suficiente que represente el riesgo real que sufre la organización y cómo ésta se puede ver afectada por el mismo.

Sin embargo, los riesgos que inicialmente fueron considerados no deben desecharse pues pueden servir para las futuras definiciones de los escenarios de riesgos. Los escenarios de riesgo generados son de utilidad al momento de analizar los riesgos.

En la generación de escenarios de riesgo se deben aplicar cuatro parámetros que forman parte de la estructura de dichos escenarios, los mismos serán útiles después para el propósito de análisis, estos son:

a) **Actor**: Es la persona o situación que hace que la amenaza explote en una vulnerabilidad, puede desenvolverse dentro o fuera de la organización, aunque no siempre será necesaria su existencia.

b) **Evento**: Es un acontecimiento o hecho inesperado que afecta las actividades dentro de la organización, en el caso de la información implicaría: pérdida, robo o divulgación de información así como daños físicos a dispositivos de almacenamiento y hardware en general. Se pueden distinguir tres tipos de evento:

1. Eventos de pérdida: Implica la ocurrencia o materialización del riesgo, es decir, que lo que se temía que pase, haya en realidad ocurrido.

Ejemplo: Un software desarrollado que no cumple con los requerimientos del usuario lo que implica pérdida de tiempo, dinero y compromete la reputación de la entidad.

2. Eventos de amenaza: Constituye la causa que desencadenó la materialización del evento de pérdida. Una amenaza puede ser: maliciosa, accidental, por error, fracaso, natural o por requerimiento externo.

Ejemplo: El usuario final presenta quejas a la entidad sobre aspectos relacionados al software recientemente implementado, pues no le sirve para cumplir con sus actividades o propósitos.

3. Eventos de vulnerabilidad: Relacionado con los controles que se manejan en la entidad, y en general, con el ambiente interno.

Ejemplo: No se definió un proceso para selección y contratación de los proveedores encargados de desarrollo e implementación de software y no se efectuaron pruebas de aceptación.

c) **Activos/recursos**: Los activos son aquellos elementos físicos de un determinado valor para la entidad mientras que los recursos son un medio para conseguir un objetivo.

Ejemplo: En el área de TI se puede emplear un sistema de enfriamiento que permita que los equipos de hardware se encuentren en óptimas condiciones para su operatividad esto constituye un activo para la entidad y a la vez un recursos porque permite alcanzar el objetivo de *MEJORAR DE LA INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN.*

d) **Tiempo**: Se describe la duración del evento relevante y el lapso de detección.

Los escenarios de riesgos genéricos sirven como una entrada para el análisis de las actividades de riesgo donde el impacto necesita ser estabilizado.

3.4.2.5. Factores de Riesgo

Para la generación de escenarios se debe considerar la influencia que tienen algunos factores de riesgos de la organización, en la frecuencia o magnitud de los eventos, como son: *los factores contextuales y las capacidades*.

El primero hace referencia al marco dentro del cual la entidad realiza sus actividades por lo tanto se encontrarán factores: internos y externos, los últimos pueden ser pocos dependiendo de la naturaleza de la empresa pero respecto a los internos estos son relativamente superiores numéricamente y con frecuencia se presentan explotando más vulnerabilidades que amenazas.

Los factores internos son manejables de manera efectiva dentro de determinadas condiciones lo que no ocurre con los factores externos, pues su ocurrencia no está en manos de la entidad sino de terceras partes y generalmente las medidas que más afectan son: económicas, desastres naturales, legales, avances apresurados de la tecnología, entre otras.

En relación a las capacidades se definen en base a la eficiencia y eficacia de las actividades en las cuales se manejan las TI. Dentro de esta se pueden identificar dos dimensiones: capacidad de gestión de riesgos y capacidades relacionadas, la primera nos permite reconocer la madurez en la realización del proceso de gestión de riesgos y en la segunda se aplican los dominios propuestos por COBIT (EDM, APO, BAI, DSS y MEA) los cuales llevan a identificar el nivel de capacidad de los procesos y otros.

En general, cuando se está desarrollando un escenario de riesgo la información que se debe tener en cuenta se basa en: el pasado, el presente y el futuro; esto implica que se debe detallar de manera clara que se entienda lo que implica la ocurrencia de determinado evento en la entidad.

CO*BTI 5 para Riegos* presenta una guía elaborada de los escenarios de riesgos genéricos, que expresan las situaciones más importantes que pueden

afectar a la organización con respecto al uso de las tecnologías y que se puede utilizar aunque se advierte que el análisis no se debe basar únicamente en esta, se menciona la capacidad de generar escenarios de riesgo propios acorde a la institución y sus necesidades.

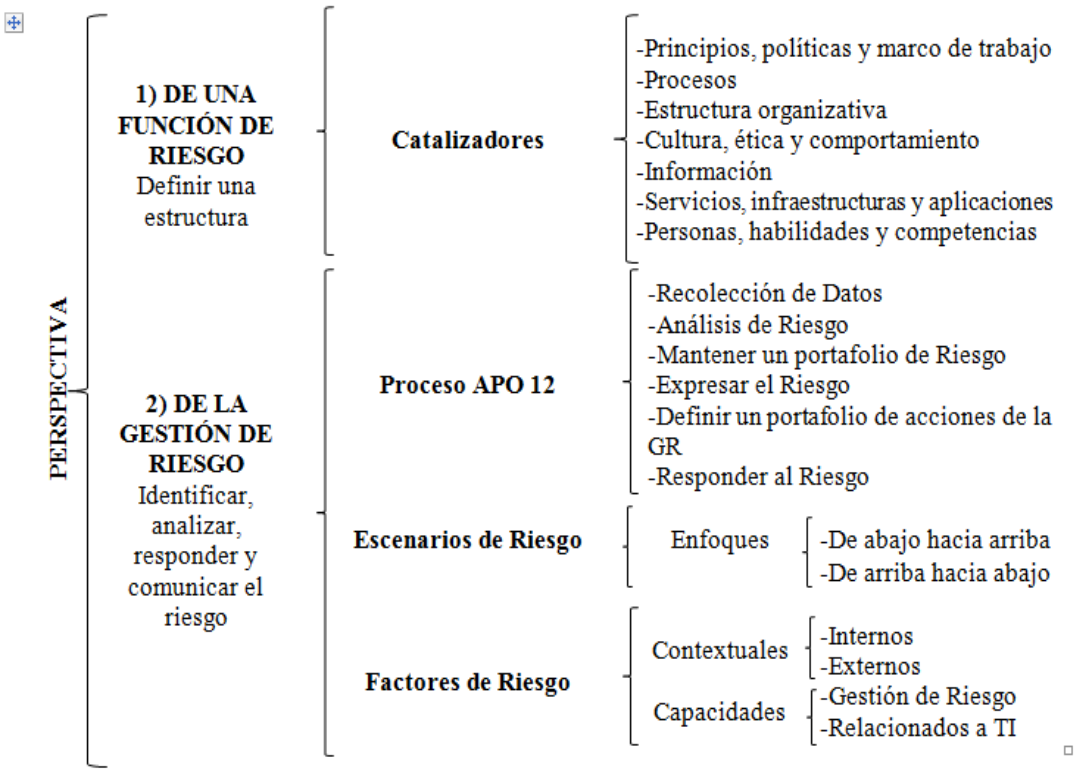


Figura 22 Síntesis de COBIT 5 para Riesgos "Perspectivas"
Fuente: (ISACA, 2013)

Para una mayor comprensión acerca de cómo COBIT 5 *para riesgos* se complementa con los diferentes estándares internacionales se presenta a continuación un esquema donde se puede apreciar que el MARCO COBIT 5 *para riesgos* abarca de manera indirecta los estándares anteriormente analizados, pero aun así este requerirá alinearse ya sea con uno o con los dos conjuntamente dependiendo de las necesidades de cada entidad para lograr una gestión óptima de los riesgos.

ETAPAS	ISO 31000	ISO 27005	COBIT 5 PARA RIESGOS
ESTABLECER UN CONTEXTO	INTERNO: Cultura, procesos, estructura y estrategias EXTERNO: Leyes, política, economía CONTEXTO: Costo, recursos, responsabilidades.	-Criterios necesarios para la gestión de riesgos para la seguridad de la información. -Determinar el alcance y límites.	-Prácticas para entender aspectos INTERNOS. -Prácticas para trabajar con aspectos EXTERNOS. -CONTEXTO de gestión de Riesgo -Desarrollo de criterios de riesgos
VALORACIÓN DEL RIESGO	-IDENTIFICACIÓN.- Por áreas, departamentos, actividades o proyectos. -ANÁLISIS.- Cuantitativo, cualitativo, impacto y probabilidad. -EVALUACIÓN.- Priorización del riesgo. Criterio del contexto versus análisis	IDENTIFICACIÓN: Bienes, amenazas, controles existentes, vulnerabilidades y consecuencias. ANÁLISIS: Valoración de las consecuencias, incidentes y niveles de riesgo. EVALUACIÓN: Niveles de riesgo versus criterios de aceptación del riesgo.	IDENTIFICACIÓN: Control, valor, amenazas y escenario de identificación de riesgo. ANÁLISIS: Estimación de los escenarios de riesgos mediante frecuencia e impacto. EVALUACIÓN: Agregación del riesgo y uso de mapa de riesgo.
TRATAMIENTO DEL RIESGO	Opciones de respuesta al riesgo: -Evitar -Incrementar -Compartir -Retener -Modificar el impacto o probabilidad	Opciones de tratamiento al riesgo: -Modificar -Retener -Evitar -Compartir	Tratamiento para los riesgos identificados: -Evitar -Reducir-Mitigar -Compartir -Aceptar
ACEPTACIÓN DEL RIESGO		Plan de tratamiento del riesgo y riesgo residual basado en costo, responsabilidad, consecuencias.	Respuesta al riesgo
MONITOREO Y REVISIÓN	Vigilancia de actividades o procesos	Continuidad para mantener una visión general de la perspectiva del riesgo.	Enfocado únicamente a resultados.
COMUNICACIÓN Y CONSULTA	Plan de comunicación	Compartir y comunicar la información con terceras partes.	Considerado como uno de los puntos primarios ya que toda la información será transmitida a los stakeholders (partes interesadas). -Plan de comunicación de riesgos -Informe de riesgos

Figura 23 Comparación de Mejores Prácticas
Fuente: Autoras

CAPÍTULO IV

METOLOGÍA PARA LA GESTIÓN DE RIESGOS

En este capítulo se conjugan los aspectos teóricos tratados en páginas anteriores aplicados a la realidad. Se emplea una metodología para el proceso de gestión de riesgos basada en los lineamientos que presenta *COBIT 5 para Riesgos* ajustada a la situación en la cual actualmente la Universidad de Cuenca se desenvuelve, pero específicamente direccionada al área encargada de las TIC conocida como Dirección de Tecnología de Información y Comunicación.

La metodología establece seis pasos resumidos en: Recopilación de Datos, Análisis del Riesgo, Mantener un Perfil del Riesgo, Expresar el Riesgo, Definición de un Portafolio de Acciones y Respuesta al Riesgo. Finalmente como resultado del análisis se obtendrá un listado de riesgos con actividades y responsables de llevar a cabo la implementación de medidas de tratamiento, aportando con un plan de mitigación para riesgos de TIC.

Daisy Fernanda Alvarado Carpio
Laura Alexandra Zumba Morales

4. METODOLOGÍA PARA LA GESTIÓN DE RIESGOS

4.1. Recopilación de Datos

4.1.1. Descripción del Ambiente Actual

La Dirección de Planificación el 08 de octubre del 2012 presentó un Plan de Mitigación de Riesgos de la Universidad de Cuenca, basado en la metodología de DMAIC, tal como se muestra en el ANEXO 1.

La información presentada en el mencionado plan, respecto a la DTIC permite conocer, entender y establecer el ámbito en el cual la Universidad ha venido desarrollando las actividades involucradas con las tecnologías de información y comunicación para lograr identificar aspectos críticos que deben ser tomados en cuenta en el proceso de gestión de riesgos.

Cabe recalcar que la Universidad de Cuenca ha definido en el Plan de Mitigación de Riesgos un proceso de evaluación para el tratamiento de sus potenciales riesgos las principales etapas desarrolladas dentro de este son las siguientes: “Contexto estratégico, Identificación de Riesgos, Análisis de riesgos, Calificación del riesgo, Valoración del riesgo, Valoración de riesgo residual, Mapa de riesgos. Finalizando con la determinación de prioridades y aplicación de respuesta ante el riesgo, comparando los niveles de riesgo detectados frente a estándares determinados”.

Sin embargo, dicho proceso ha sido aplicado de manera general en la Universidad, hecho que se diferencia de la realización de este trabajo, cuyo enfoque se centra en las Tecnologías de la Información y Comunicación manejadas por la DTIC y su importancia para mejorar el desempeño institucional.

Para complementar lo conocido anteriormente, se procede a la identificación de la diversidad de riesgos externos que pueden afectar a la entidad, pero para el presente trabajo se han considerado únicamente aquellos relacionados con las actividades cotidianas, las cuales se ven influenciadas por una normativa legal vigente.

El incumplimiento de alguna de las normas presentadas en la Norma de Control Interno para entidades y organismos del sector público y las personas jurídicas de derecho privado que dispongan de recursos públicos puede implicar el incremento de los riesgos que no han sido cubiertos de manera adecuada por los controles internos fijados.

De acuerdo a dicha normativa y con base únicamente a la norma 410: Tecnología de la Información se han identificado en general los siguientes riesgos:

- Descoordinación de funciones, actividades y responsabilidades relacionadas con TI que con llevan a realizar actividades duplicadas y no fructíferas que imposibilitan el cumplimiento de los objetivos tanto de la DTIC así como los institucionales.
- Carecer de una adecuada administración de proyectos tecnológicos, lo cual implica la probabilidad de que ocurran pérdidas a nivel de recursos tecnológicos, monetarios y tiempo. Además tiene un impacto importante al momento de generar valor agregado mediante el uso de las tecnologías informáticas, ya que puede disminuir la cantidad y calidad de los servicios ofrecidos.
- Fallas en la toma de decisiones en cuanto a identificar y establecer los requerimientos de un software en relación con las necesidades de un usuario que a su vez influye en decidir, si este puede ser desarrollado o adquirido.
- Fallas en la adquisición, mantenimiento y control de la infraestructura tecnológica debido a la descoordinación en los contratos con proveedores ya sea de hardware o software.
- Falencias en la administración de seguridad permanente de aquellos accesos vulnerables tanto a nivel físico como de la información crítica, el desconocimiento o desactualización de los mismos causa brechas en la determinación de planes de contingencias.
- Insatisfacción de los usuarios internos o externos debido a la ausencia de monitoreo, supervisión y evaluación de procesos y servicios; es

decir, desactualización de los indicadores que muestran la realidad frente a lo inicialmente planteado.

- Personal desactualizado en áreas importantes dentro de la DTIC tales como: soporte técnico, mantenimiento y protección de equipos entre otras; lo cual repercute directamente a las capacidades institucionales.
- Descoordinación en las actividades y toma de decisiones así como en la definición de políticas debido a la inexistencia de un comité informático el cual sirva de soporte y apoyo para la DTIC.

En este punto, se ha obtenido un conocimiento global de los riesgos a los que está expuesta la DTIC, identificando aquellos aspectos claves en los cuales pueden existir falencias.

4.1.2. Priorización de procesos

4.1.2.1. Identificación de los objetivos institucionales

La Universidad de Cuenca busca incrementar el nivel de eficiencia de la gestión académica y administrativa, para ello se ha propuesto la implementación de un modelo basado en procesos el cual se encuentra detallado en el Plan Estratégico Institucional 2012-2017.

El enfoque por procesos se menciona en el conjunto de la ISO 9000 como uno de los siete principios para la gestión de la calidad. Sostiene que la entidad puede lograr sus objetivos de manera eficaz considerando todo como un proceso, es decir, cada actividad y recurso que maneje la entidad se enfoca únicamente en los resultados que se logren.

El modelo permite el uso y aplicación a la par del concepto de *mejora continua,* que debe estar presente de forma latente en la entidad para asegurar que genera valor agregado así como mantener su nivel operativo y competitivo dentro del ámbito en el cual se ubica.

Para iniciar el cambio de enfoque la Universidad realizó un mapa de procesos que constituye una representación gráfica de la estructura de procesos del

sistema de gestión, este es similar al modelo planteado por ISO, pero adecuado a su realidad, en el cual se ubica a las actividades relacionadas a la dirección de TIC dentro de los denominados *procesos habilitantes de apoyo.*

Como se identificó en el capítulo uno, la Universidad cuenta con dieciocho objetivos de gestión institucional, si bien se mencionan otros por los restantes tres ejes institucionales, los mismos que sirven de base para poder iniciar el *proceso de gestión de riesgos*.

Los objetivos se encuentran encaminados principalmente al mejoramiento de la prestación de los servicios así como a la administración de las tecnologías. De los objetivos globales se tomaron únicamente aquellos relacionados con Tecnología de la Información y Comunicación considerados dentro del eje de *gestión institucional.*

4.1.2.2. Identificación de los objetivos de la DTIC

Se requiere conocer concretamente cada uno de los objetivos que persigue la DTIC, que son los planteados inicialmente en el Plan Estratégico Institucional 2012-2017, ya que posteriormente servirán para la identificación de los procesos relacionados planteados en COBIT 5.

A continuación se detallan de manera global cada objetivo:

1) *Fortalecer la estructura organizacional de la Dirección de Desarrollo Informático (ahora DTIC)*

Este fortalecimiento se basa principalmente en brindar la capacitación idónea al personal de TIC, así como el establecimiento de metodologías para el desarrollo, mantenimiento e implementación de software y estructuras del departamento.

2) *Automatizar los procesos de la Universidad de Cuenca*

Las acciones se direccionan a la administración, coordinación, mantenimiento, mejoramiento y seguimiento de los diversos sistemas de gestión implementados,

así como también la integración de la página web de la universidad y demás sitios web para móviles.

Dentro de la automatización también se contempla la compra de licencias de archivos PDF, el control de fechas y herramientas relacionadas con un contrato.

3) Mejorar progresivamente la prestación de servicios informáticos

Consiste en la implementación de software de gestión de servicios del departamento y sistemas de almacenamiento. La creación de clúster de servidores para la prestación de servicios tanto de portales web como del entorno virtual de educación.

4) Mejora de la infraestructura de tecnologías de información y comunicación

Implica considerar todos aquellos aspectos que permitan la protección y salvaguarda de la información mediante sistemas de respaldos, cambios oportunos de computadoras o equipos en general que se encuentren en mal estado entre otros aspectos relacionados.

OBJETIVOS ESTRATÉGICOS	RAZÓN DE SER			
	FORTALECIMIENTO INSTITUCIONAL	Ciencia Tecnología e Innovación		
		Docencia		
		Vinculación con la colectividad		
		Incrementar el nivel de eficiencia de la gestión académica y administrativa acorde al nuevo modelo de generación y gestión del conocimiento y del modelo de gestión de procesos	Gestión institucional	Objetivos relacionados con TIC 1.-Fortalecer la Estructura Organizacional de la Dirección de Desarrollo de Informático (DDI). 2.-Automatizar los procesos de la Universidad de Cuenca. 3.-Mejorar Progresivamente la calidad de la prestación de servicios informáticos. 4. Mejoramiento de la infraestructura de TI.

Figura 24 Objetivos institucionales y de la DTIC
Fuente: Plan Estratégico de la Universidad de Cuenca 2014, Código: UC-DIPUC-PL-09

Objetivos Estratégicos de DTIC

4.1.2.3. Asociación con metas corporativas

Con los objetivos de la DTIC identificados se procede a determinar cuáles son las metas corporativas genéricas de las presentadas por COBIT 5 con las que se relacionan, teniendo en cuenta que la mayoría de metas pertenecientes a una empresa pueden ser mapeadas fácilmente con una o más metas genéricas.

Dimensión de CMI	Meta Corporativa
Financiera	1. Valor para las partes interesadas de las inversiones de Negocio
	2. Cartera de productos y servicios competitivos
	3. Riesgos de negocio gestionados (salvaguarda de activos)
	4. Cumplimiento de Leyes y regulaciones externas
	5. Transparencia financiera
Cliente	6. Cultura de servicio orientada al cliente
	7. Continuidad y disponibilidad del servicio de negocio
	8. Respuestas ágiles a un entorno de negocio cambiante
	9. Toma estratégica de decisiones basada en información
	10. Optimización de costes de entrega del servicio
Interna	11. Optimización de la funcionalidad de los procesos de negocio
	12. Optimización de los costes de los procesos de negocio
	13. Programas gestionados de cambio en el negocio
	14. Productividad operacional y de los empleados
	15. Cumplimiento con las políticas internas
Aprendizaje	16. Personas preparadas y motivadas
	17. Cultura de innovación de producto negocio

Figura 25 Metas Corporativas de COBIT 5
Fuente: (ISACA, 2012)

Las metas corporativas genéricas de *COBIT 5* están basadas en las cuatro dimensiones planteadas por el denominado cuadro de mando integral BSC: *Balance Score Card,* se detalla una lista de metas buscadas habitualmente por las empresas en relación al negocio y a las cuales una entidad o empresa puede adaptarse.

El cuadro de mando integral hace referencia a una herramienta técnica que maneja las funciones y procesos de las tecnologías, no se enfoca únicamente en la parte financiera sino más bien relaciona a la misma con otras partes como: clientes, proceso y aprendizaje que se interrelacionan, esto permite conseguir el alineamiento de las TIC con la organización en general. Esta herramienta es útil para el mediano o largo plazo por el uso de indicadores financieros, no financieros y de control.

Las cuatro dimensiones manejadas para las metas corporativas y de TIC, engloban lo siguiente:

a) *FINANCIERA:* Recoge aspectos relacionados al fin último perseguido por los accionistas de *maximizar los beneficios* de sus inversiones y con ello relacionando costes y optimización.

b) *CLIENTE:* Relacionada con el nivel de satisfacción del cliente/usuario de la entidad.

c) *INTERNA:* Relacionada con la funcionalidad, productividad, procesos, normativa y demás que constituyen el ambiente en el cual opera la entidad.

d) *APRENDIZAJE Y CRECIMIENTO:* La primera relacionada con las personas que constituyen uno de los elementos más importantes dentro de la entidad y el segundo hace referencia a la tecnología que permite el desarrollo de actividades a un mayor nivel.

Ejemplo:

Objetivo N° 1: Fortalecer la estructura organizacional de la Dirección de Tecnologías de Información y Comunicación

Al mapear las metas corporativas genéricas con respecto al objetivo de la DTIC se determinó, que la meta más acorde con dicho objetivo por facilitar su consecución es la número 14: *PRODUCTIVIDAD OPERACIONAL Y DE LOS EMPLEADOS* .

Dimensión de CMI	Meta Corporativa
Financiera	1. Valor para las partes interesadas de las inversiones de Negocio
	2. Cartera de productos y servicios competitivos
	3. Riesgos de negocio gestionados (salvaguarda de activos)
	4. Cumplimiento de Leyes y regulaciones externas
	5. Transparencia financiera
Cliente	6. Cultura de servicio orientada al cliente
	7. Continuidad y disponibilidad del servicio de negocio
	8. Respuestas ágiles a un entorno de negocio cambiante
	9. Toma estratégica de decisiones basada en información

	10. Optimización de costes de entrega del servicio
Interna	11. Optimización de la funcionalidad de los procesos de negocio
	12. Optimización de los costes de los procesos de negocio
	13. Programas gestionados de cambio en el negocio
	14. Productividad operacional y de los empleados
	15. Cumplimiento con las políticas internas
Aprendizaje	16. Personas preparadas y motivadas
	17. Cultura de innovación de producto negocio

Figura 26 Metas Corporativas de COBIT 5 OE1
Fuente: **(**ISACA**,** 2012**)**

La estructura organizacional se refiere al ámbito interno dentro del cual la entidad va realizar sus actividades, por ello se considera la elección de una de las cinco metas corporativas ubicada dentro de la dimensión del CMI: *INTERNA,* ya que permite alcanzar la optimización de los recursos y a la vez generar beneficios para las partes interesadas.

La productividad del área de TI dependerá de: las distintas situaciones relacionadas a competencias y habilidades de su personal pues los empleados preparados y competentes permitirán cubrir las necesidades tanto institucionales y de terceros incrementando su nivel en la entrega de beneficios; así como también de la efectividad en la definición y ejecución de procesos primarios o críticos de la entidad.

Recordando los dos proyectos planteados por la DTIC, se puede vincular estos con la meta corporativa seleccionada así: la *implementación de la metodología para el desarrollo, mantenimiento y/o adquisición de software y estructura del centro de desarrollo de software* se enmarca en la productividad operacional ya que brinda un marco referente acerca de cómo realizar actividades y procesos, teniendo en cuenta aspectos relevantes como tiempo, personas y recursos; a través de un serie de pasos o etapas que favorecen la optimización.

Por el lado del personal se plantea un *Plan de Capacitación del personal de TIC* acción que repercute en la productividad del personal respecto de su capacidad para llevar a cabo sus tareas.

Objetivo N°2: Automatizar los procesos de la Universidad de Cuenca

De igual manera para este objetivo se identifican las siguientes metas corporativas genéricas que favorecen su cumplimiento: N°11: *OPTIMIZACIÓN DE LA FUNCIONALIDAD DE LOS PROCESOS DE NEGOCIO*, N° 12 *OPTIMIZACIÓN DE LOS COSTES DE LOS PROCESOS DE NEGOCIO*, N° 14: *PRODUCTIVIDAD OPERACIONAL Y DE LOS EMPLEADOS*.

Dimensión de CMI	Meta Corporativa
Financiera	1. Valor para las partes interesadas de las inversiones de Negocio
	2. Cartera de productos y servicios competitivos
	3. Riesgos de negocio gestionados (salvaguarda de activos)
	4. Cumplimiento de Leyes y regulaciones externas
	5. Transparencia financiera
Cliente	6. Cultura de servicio orientada al cliente
	7. Continuidad y disponibilidad del servicio de negocio
	8. Respuestas ágiles a un entorno de negocio cambiante
	9. Toma estratégica de decisiones basada en información
	10. Optimización de costes de entrega del servicio
Interna	11. Optimización de la funcionalidad de los procesos de negocio
	12. Optimización de los costes de los procesos de negocio
	13. Programas gestionados de cambio en el negocio
	14. Productividad operacional y de los empleados
	15. Cumplimiento con las políticas internas
Aprendizaje y Crecimiento	16. Personas preparadas y motivadas
	17. Cultura de innovación de producto negocio

Figura 27 Metas Corporativas de COBIT 5 OE2
Fuente: (ISACA, 2012)

Las tres metas corporativas se ubican dentro de la dimensión del CMI denominado INTERNA, anteriormente definida. La automatización de los diversos procesos definidos en el *Mapa de Procesos* de la entidad dependerá de la administración y gestión interna global así como de cada una de las áreas para su consecución.

Para lograr una automatización de procesos se vuelve primordial cumplir las especificaciones inicialmente planteadas, en el respectivo manual, en el menor tiempo posible con un porcentaje mínimo de intentos (hablamos de la

funcionalidad), teniendo en cuenta que ello ocasiona la optimización de los recursos que se manejan a nivel material o financiero en el cual se considera a la inversión planificada como requisito indispensable para el establecimiento de prioridades, de tal manera que se favorezca el incremento de la productividad operacional así como del personal.

Respecto de los proyectos que han sido planteados por la DTIC se destacan varios relacionados al manejo o implementación de *Sistemas de Gestión* esto es muy importante, ya que *cada vez más, las empresas se enfrentan a demandas de rentabilidad, calidad y tecnología que contribuyan al desarrollo sostenible. Un sistema de gestión eficiente le puede ayudar a convertir esas presiones en una ventaja competitiva.* (DNV-GL, 2015)

Conjuntamente con los proyectos complementarios, la entidad puede automatizar los procesos pero teniendo en cuenta la funcionalidad de estos así como de costes y personal involucrado de manera que se logre el máximo beneficio. En resumen, las tres metas seleccionadas direccionan los esfuerzos y recursos al logro del OE N°2.

Objetivo N°3: Mejorar progresivamente la prestación de servicios informáticos

Para el tercer objetivo se señalan a continuación las metas que apoyan a su realización:

Dimensión de CMI	Meta Corporativa
Financiera	1. Valor para las partes interesadas de las inversiones de Negocio
	2. Cartera de productos y servicios competitivos
	3. Riesgos de negocio gestionados (salvaguarda de activos)
	4. Cumplimiento de Leyes y regulaciones externas
	5. Transparencia financiera
Cliente	6. Cultura de servicio orientada al cliente
	7. Continuidad y disponibilidad del servicio de negocio
	8. Respuestas ágiles a un entorno de negocio cambiante
	9. Toma estratégica de decisiones basada en información
	10. Optimización de costes de entrega del servicio

Interna	11. Optimización de la funcionalidad de los procesos de negocio
	12. Optimización de los costes de los procesos de negocio
	13. Programas gestionados de cambio en el negocio
	14. Productividad operacional y de los empleados
	15. Cumplimiento con las políticas internas
Aprendizaje y Crecimiento	16. Personas preparadas y motivadas
	17. Cultura de innovación de producto negocio

Figura 28 Metas Corporativas de COBIT 5 OE3
Fuente: (ISACA, 2012)

Las metas corporativas seleccionadas para soportar el OE pertenecen a la dimensión CLIENTE, debido a que la entidad debe enfocarse en lo que el cliente necesita y requiere de los servicios prestados por la institución en relación con la interacción virtual a través de los distintos medios manejados, direccionados al uso de: profesores, alumnos, personal así como personas externas en general.

Las metas se centran en mantener comportamientos, valores (institucionales como del personal) y todos los elementos relacionados a la cultura organizacional enfocadas en satisfacer al cliente dentro de la capacidad y razón de ser de la entidad. Este aspecto se vuelve fundamental ya que permite diferenciar a la entidad de otras, pues la calidad de los servicios en aspectos claves como tiempo y funcionalidad será considerada por el cliente y realzará la imagen institucional.

Adicionalmente a estos aspectos se considera necesario que la entidad mantenga la *continuidad y disponibilidad* de sus servicios, lo cual se puede traducir en la implementación de un Plan de Continuidad del Negocio que se convierte en una herramienta de acción que guía el actuar de la entidad cuando un determinado acontecimiento sucede y sus servicios se ven directamente afectados, resumidamente actúa como el plan B.

Respecto de los planes que la institución maneja se destacan: aplicación de encuestas por medio de la aplicación denominada LimeSurvey, la capacitación para la administración de Servicios de Redes y Comunicaciones así como implementación de distintas plataformas.

Sin embargo, se debe mencionar que los demás proyectos se vuelven secundarios al OE y no logran apalancar los resultados deseados, por ende debería ser objeto de análisis para mejorar estos o generar nuevos, enfocados a la continuidad de los servicios.

Objetivo N°4: Mejoramiento de la infraestructura de TIC

Las metas corporativas identificadas para este objetivo son N°8: *RESPUESTAS ÁGILES A UN ENTORNO DE NEGOCIO CAMBIANTE*, N°9: *TOMA ESTRATÉGICA DE DECISIONES BASADA EN INFORMACIÓN*, N°:10 *OPTIMIZACIÓN DE COSTES DE ENTREGA DEL SERVICIO* y N° 15: *CUMPLIMIENTO CON LAS POLÍTICAS INTERNAS.*

Dimensión de CMI	Meta Corporativa
Financiera	1. Valor para las partes interesadas de las inversiones de Negocio
	2. Cartera de productos y servicios competitivos
	3. Riesgos de negocio gestionados (salvaguarda de activos)
	4. Cumplimiento de Leyes y regulaciones externas
	5. Transparencia financiera
Cliente	6. Cultura de servicio orientada al cliente
	7. Continuidad y disponibilidad del servicio de negocio
	8. Respuestas ágiles a un entorno de negocio cambiante
	9. Toma estratégica de decisiones basada en información
	10. Optimización de costes de entrega del servicio
Interna	11. Optimización de la funcionalidad de los procesos de negocio
	12. Optimización de los costes de los procesos de negocio
	13. Programas gestionados de cambio en el negocio
	14. Productividad operacional y de los empleados
	15. Cumplimiento con las políticas internas
Aprendizaje y Crecimiento	16. Personas preparadas y motivadas
	17. Cultura de innovación de producto negocio

Figura 29 Metas Corporativas de COBIT 5 OE4
Fuente: (ISACA, 2012)

La dimensión CLIENTE (en el caso de la universidad definido como *usuario*) fue considerada debido a que la entidad debe planificar todas las actividades relacionadas a la adquisición, renovación, mejora o complementación de la infraestructura de TIC basados en las exigencias tanto del usuario como del

entorno en cual se desenvuelven teniendo en cuenta el manejo de presupuestos que se fundamenten en un análisis de costos que contemple una diversidad de alternativas que permitan la satisfacción del cliente pero, administrando adecuadamente los recursos asignados para la ejecución del programa o proyecto.

Consecuentemente, la información obtenida tanto de los requerimientos o expectativas del cliente así como de las diversas propuestas analizadas y cualquier otro tipo de información complementaria relacionada facilita la toma de decisiones oportunas.

Por otro lado, la dimensión INTERNA se relaciona con las políticas estipuladas por la DTIC que constituyen directrices que se deben considerar previamente al momento de ejecutar temas relacionados con la adquisición tanto de los activos tecnológicos y equipos informáticos como de los programas informáticos. Sin embargo, para aspectos relacionados con el manejo de datos mediante respaldos o sistemas existen políticas específicas de TI dependiendo el caso.

Las metas corporativas seleccionadas se relacionan y soportan los proyectos plateados por la DTIC referentes principalmente a varias adquisiciones e implementación de quipos y herramientas informáticas en general necesarias para brindar servicios con lo último en tecnología dentro de su capacidad.

4.1.2.4. Identificación de las metas de TI

Una vez identificadas las metas genéricas relacionadas con la empresa se procede a identificar su correspondencia con las metas de las tecnologías de información (TI) que incluye tanto los datos, sistemas y procesos de información. *COBIT 5* propone diecisiete metas relacionadas con las tecnologías de información con las cuales se deberá mapear. Ver ANEXO 2.

Ejemplo:

Objetivo N°1: Fortalecer la estructura organizacional de la DTIC

Metas relacionadas con TI			1. Valor para las partes interesadas de las inversiones de Negoci	2. Cartera de productos y servicios competitivos	3. Riesgos de negocio gestionados (salvaguarda de activos)	4. Cumplimiento de Leyes y regulaciones externas	5. Transparencia financiera	6. Cultura de servicio orientada al cliente	7. Continuidad y disponibilidad del servicio de negocio	8. Respuestas ágiles a un entorno de negocio cambiante	9. Toma estratégica de decisiones basada en información	10. Optimización de costes de entrega del servicio	11. Optimización de la funcionalidad de los procesos de negoci	12. Optimización de los costes de los procesos de negocio	13. Programas gestionados de cambio en el negocio	14. Productividad operacional y de los empleados	15. Cumplimiento con las políticas internas	16. Personas preparadas y motivadas	17. Cultura de innovación de producto negocio
Financiera	1	Alineamiento de TI y estrategia del negocio	P	P	S			P	S	P	P	S	P	S	P			S	S
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio, de las leyes y regulaciones externas			S	P											P		
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S					S	S		S		P			S	S
	4	Riesgos de negocio relacionados con las TI gestionados			P	S			P	S		P			S		S	S	
	5	Realización de beneficios de portafolio de inversiones y servicios relacionados con las TI	P	P				S		S		S	S	P		S			S
	6	Transparencia de los costes, beneficios y riesgos de la TI	S		S		P				S	P		P					
Cliente	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Interno	9	Agilidad de las TI	S	P	S			S		P			P		S	S		S	P
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones			P	P			P								P		
	11	Optimización de activos, recursos y capacidades de la TI	P	S						S		P	S	P	S	S			S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones en procesos de negocio	S	P	S			S		S		S	P	S	S	S			S
	13	Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los	P	S	S			S				S		S	P				
	14	Disponibilidad de información útil y relevante para la toma de decisiones	S	S	S	S			P		P		S						
	15	Cumplimiento de TI con las políticas internas			S	S											P		
Aprendizaje y crecimiento	16	Personal del negocio y de las TI competente y motivado	S	S	P			S		S						P		P	S
	17	Conocimiento, experiencia e iniciativas para la innovación del negocio	S	P				S		P	S		S		S			S	P

Figura 30 Mapeo entre las Metas Corporativas de COBIT 5 y las Metas relacionadas con las TI
Fuente: (ISACA, 2012)

Nos ubicamos en el área de *METAS CORPORATIVAS* buscando la meta de la DTIC catorce anteriormente seleccionada al seguir de forma descendente podemos observar *METAS DE TI* primarias y secundarias, de ellas se eligen las primarias “P” por que apoyan de manera total a la meta corporativa y las secundarias sirven de apoyo.

Las *METAS DE TI* seleccionadas son de la dimensión CLIENTE N° 08: Uso adecuado de aplicaciones información y soluciones tecnológicas; y de la dimensión APRENDIZAJE Y CRECIMIENTO N° 16: Personal de negocio de las TI competente y motivado que son las más relevantes para el cumplimiento del objetivo analizado.

Objetivo N°2: Automatizar los procesos de la Universidad de Cuenca

Metas relacionadas con TI			1. Valor para las partes interesadas de las inversiones de Negoci	2. Cartera de productos y servicios competitivos	3. Riesgos de negocio gestionados (salvaguarda de activos)	4. Cumplimiento de Leyes y regulaciones externas	5. Transparencia financiera	6. Cultura de servicio orientada al cliente	7. Continuidad y disponibilidad del servicio de negocio	8. Respuestas ágiles a un entorno de negocio cambiante	9. Toma estratégica de decisiones basada en información	10. Optimización de costes de entrega del servicio	11. Optimización de la funcionalidad de los procesos de negoci	12. Optimización de los costes de los procesos de negocio	13. Programas gestionados de cambio en el negocio	14. Productividad operacional y de los empleados	15. Cumplimiento con las políticas internas	16. Personas preparadas y motivadas	17. Cultura de innovación de producto negocio
Financiera	1	Alineamiento de TI y estrategia del negocio	P	P	S			P	S	P	P	S	P	S	P			S	S
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio, de las leyes y regulaciones externas			S	P											P		
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S					S	S		S		P			S	S
	4	Riesgos de negocio relacionados con las TI gestionados			P	S			P	S		P			S		S	S	
	5	Realización de beneficios de portafolio de inversiones y servicios relacionados con las TI	P	P				S		S		S	S	P		S			S
	6	Transparencia de los costes, beneficios y riesgos de la TI	S		S		P				S	P		P					
Cliente	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Interno	9	Agilidad de las TI	S	P	S			S		P			P		S	S		S	P
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones			P	P			P								P		
	11	Optimización de activos, recursos y capacidades de la TI	P	S						S		P	S	P	S	S			S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones en procesos de negocio	S	P	S			S		S		S	P	S	S	S			S
	13	Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los	P	S	S			S				S		S	P				
	14	Disponibilidad de información útil y relevante para la toma de decisiones	S	S	S	S			P		P		S						
	15	Cumplimiento de TI con las políticas internas			S	S											P		
Aprendizaje y crecimiento	16	Personal del negocio y de las TI competente y motivado	S	S	P			S		S						P		P	S
	17	Conocimiento, experiencia e iniciativas para la innovación del negocio	S	P				S		P	S		S		S			S	P

Figura 31 Mapeo entre las Metas Corporativas de COBIT 5 y las Metas relacionadas con las TI OE2
Fuente: (ISACA, 2012)

Las *METAS DE TI* seleccionadas para la *META CORPORATIVA* N°11 son de la dimensión FINANCIERA N°01: Alineamiento de TI y estrategia del negocio; de la dimensión CLIENTE N°7: Entrega de servicios de TI de acuerdo a los requisitos del negocio y N°8: Uso adecuado de aplicaciones, información y

soluciones tecnológicas; y para la dimensión; INTERNA N°9: Agilidad de las TI, N°12: Capacitación y soporte de procesos de negocio integrando aplicaciones en procesos de negocios.

Por otro lado, la *META CORPORATIVA* N°12 se relaciona con *METAS DE TI* contempladas dentro de las siguientes dimensiones:

- FINANCIERA.- N° 5: Realización de beneficios del portafolio de inversiones y servicios relacionados con las TI y N°6: Transparencia de los costos beneficios y riesgos de la TI.
- INTERNA.- N°11: Optimización de activos, recursos y capacidades de la TI.

Por otro lado, la *META CORPORATIVA* N°14 se relaciona con *METAS DE TI* contempladas dentro de las siguientes dimensiones:

- CLIENTE.- N°8: Uso adecuado de aplicaciones, información y soluciones tecnológicas;
- APRENDIZAJE Y CRECIMIENTO.- N° 16: Personal del negocio y de las TI competente y motivado.

Objetivo N°3: Mejorar progresivamente la calidad de la prestación de servicios informáticos

Metas relacionadas con TI			1. Valor para las partes interesadas de las inversiones de Negoci	2. Cartera de productos y servicios competitivos	3. Riesgos de negocio gestionados (salvaguarda de activos)	4. Cumplimiento de Leyes y regulaciones externas	5. Transparencia financiera	6. Cultura de servicio orientada al cliente	7. Continuidad y disponibilidad del servicio de negocio	8. Respuestas ágiles a un entorno de negocio cambiante	9. Toma estratégica de decisiones basada en información	10. Optimización de costes de entrega del servicio	11. Optimización de la funcionalidad de los procesos de negoci	12. Optimización de los costes de los procesos de negocio	13. Programas gestionados de cambio en el negocio	14. Productividad operacional y de los empleados	15. Cumplimiento con las políticas internas	16. Personas preparadas y motivadas	17. Cultura de innovación de producto negocio
Financiera	1	Alineamiento de TI y estrategia del negocio	P	P	S			P	S	P	P	S	P	S	P			S	S
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio, de las leyes y regulaciones externas			S	P											P		
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S					S	S		S		P			S	S
	4	Riesgos de negocio relacionados con las TI gestionados			P	S			P	S		P			S		S	S	
	5	Realización de beneficios de portafolio de inversiones y servicios relacionados con las TI	P	P				S		S		S	S	P		S			S
	6	Transparencia de los costes, beneficios y riesgos de la TI	S		S		P				S	P		P					
Cliente	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Interno	9	Agilidad de las TI	S	P	S			S		P			P		S	S		S	P
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones			P	P			P								P		
	11	Optimización de activos, recursos y capacidades de la TI	P	S						S		P	S	P	S	S			S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones en procesos de negocio	S	P	S			S		S		S	P	S	S	S			S
	13	Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los	P	S	S			S				S		S	P				
	14	Disponibilidad de información útil y relevante para la toma de decisiones	S	S	S	S			P		P		S						
	15	Cumplimiento de TI con las políticas internas			S	S											P		
Aprendizaje y crecimiento	16	Personal del negocio y de las TI competente y motivado	S	S	P			S		S						P		P	S
	17	Conocimiento, experiencia e iniciativas para la innovación del negocio	S	P				S		P	S		S		S			S	P

Figura 32 Mapeo entre las Metas Corporativas de COBIT 5 y las Metas relacionadas con las TI OE3

Fuente: (ISACA, 2012)

Las *METAS DE TI* seleccionadas para la *META CORPORATIVA* N°6 son de la dimensión FINANCIERA N°01: Alineamiento de TI y estrategia del negocio; mientras que para la dimensión CLIENTE se prioriza la N°7: Entrega de servicios de TI de acuerdo a los requisitos del negocio.

En relación con la *META CORPORATIVA* N°7 las metas relacionadas se ubican en la dimensión FINANCIERA N°4 Riesgos de negocio relacionados con las TI gestionados y para la dimensión INTERNA se ubican dos: N°10 Seguridad de la información, infraestructura de procesamiento y aplicaciones y N°14 Disponibilidad de información útil y relevante para la toma de decisiones.

Objetivo N°4: Mejoramiento de la infraestructura de TIC

Metas relacionadas con TI			1. Valor para las partes interesadas de las inversiones de Negoci	2. Cartera de productos y servicios competitivos	3. Riesgos de negocio gestionados (salvaguarda de activos)	4. Cumplimiento de Leyes y regulaciones externas	5. Transparencia financiera	6. Cultura de servicio orientada al cliente	7. Continuidad y disponibilidad del servicio de negocio	8. Respuestas ágiles a un entorno de negocio cambiante	9. Toma estratégica de decisiones basada en información	10. Optimización de costes de entrega del servicio	11. Optimización de la funcionalidad de los procesos de negoci	12. Optimización de los costes de los procesos de negocio	13. Programas gestionados de cambio en el negocio	14. Productividad operacional y de los empleados	15. Cumplimiento con las políticas internas	16. Personas preparadas y motivadas	17. Cultura de innovación de producto negocio
Financiera	1	Alineamiento de TI y estrategia del negocio	P	P	S			P	S	P	P	S	P	S	P			S	S
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio, de las leyes y regulaciones externas			S	P											P		
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S					S	S		S		P			S	S
	4	Riesgos de negocio relacionados con las TI gestionados			P	S			P	S		P			S		S	S	
	5	Realización de beneficios de portafolio de inversiones y servicios relacionados con las TI	P	P				S		S		S	S	P		S			S
	6	Transparencia de los costes, beneficios y riesgos de la TI	S		S		P				S	P		P					
Cliente	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Interno	9	Agilidad de las TI	S	P	S			S		P			P		S	S		S	P
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones			P	P			P								P		
	11	Optimización de activos, recursos y capacidades de la TI	P	S						S		P	S	P	S	S			S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones en procesos de negocio	S	P	S			S		S		S	P	S	S	S			S
	13	Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los	P	S	S			S				S		S	P				
	14	Disponibilidad de información útil y relevante para la toma de decisiones	S	S	S	S			P		P		S						
	15	Cumplimiento de TI con las políticas internas			S	S											P		
Aprendizaje y crecimiento	16	Personal del negocio y de las TI competente y motivado	S	S	P			S		S						P		P	S
	17	Conocimiento, experiencia e iniciativas para la innovación del negocio	S	P				S		P	S		S		S			S	P

Figura 33 Mapeo entre las Metas Corporativas de COBIT 5 y las Metas relacionadas con las TI OE4

Fuente: (ISACA, 2012)

Para el cuarto objetivo, la *META CORPORATIVA* N°8 se relaciona con *METAS DE TI* contempladas dentro de las siguientes dimensiones:

- FINANCIERA: N°1: Alineamiento de TI y estrategia del negocio
- CLIENTE.- N°7: Entrega de servicios de TI de acuerdo a los requisitos del negocio
- INTERNA.- N°9: Agilidad de las TI
- APRENDIZAJE Y CRECIMIENTO.- N°17: Conocimiento, experiencia e iniciativa para la innovación del negocio.

La *META CORPORATIVA* N°9 se relaciona con *METAS DE TI* contempladas dentro de las siguientes dimensiones:

- FINANCIERA: N°1: Alineamiento de TI y estrategia del negocio
- INTERNA.- N°14: Disponibilidad de información útil y relevante para la toma de decisiones.

La *META CORPORATIVA* N°10 se relaciona con *METAS DE TI* contempladas dentro de las siguientes dimensiones:

- FINANCIERA.- N°4: Riesgos de negocio relacionados con las TI gestionados y N°6: Transparencia de los costos beneficios y riesgos de la TI.
- INTERNA.- N°11: Optimización de activos, recursos y capacidades de la TI.

Concluyendo así con la *META CORPORATIVA* N°15 se relaciona con *METAS DE TI* contempladas dentro de las siguientes dimensiones:

- FINANCIERA: N°2: Cumplimiento y soporte de la TI al cumplimiento del negocio, de las leyes y regulaciones externas.
- INTERNA.- N°10: Seguridad de la información, estructura de procesamiento y aplicaciones.

Todas las METAS DE TI mapeadas guardan una estrecha relación con los objetivos planteados tanto por la DTIC como por la entidad. Además, las diferentes metas planteadas por COBIT 5 se pueden adaptar, si se requiere, sin necesidad de cambios complejos.

4.1.2.5. Identificación de los procesos

Para cada una de las metas de TI se propone un conjunto de procesos que pueden aportar de manera muy significativa a la consecución del objetivo pero se distinguen entre primarios y secundarios. Ver ANEXO 3.

Ejemplo:

Objetivo N°1: Fortalecer la estructura organizacional de la DTIC

		Procesos deCOBIT 5	01 Alineamiento de TI y la estrategia de negocio	02 Cumplimiento y soporte de la TI al cumplimiento del negocio las leyes y las regulaciones externas	03 Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	04 Riesgos de negocio relacionados con las TI gestionados	05 Realizacion de beneficios del portafolio de Inversiones y Servicios relacionados con TI	06 Transparencia de los costes, beneficios y riesgos de TI	07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	08 Uso adecuado de aplicaciones, informacion y soluciones tecnologicas	09 Agilidad de las TI	10 Seguridad de la Informacion, infraestructura de procesamiento y aplicaciones	11 Optimizacion de activos, recursos y capacidades de las TI	12 Capacitacion y soporte de procesos de negocio integrando aplicaciones y tecnologia en procesos de negocio	13 Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	14 Disponibilidad de informacion util y relevante para la toma de decisiones	15 Cumplimiento de las politicas internas por parte de las TI	16 Personal del negocio y de las TI competente y motivado	17 Conocimiento, experiencia e iniciativas para la innovacion de negocio
			Financiera						Cliente		Interna								Aprendizaje y crecimiento	
Evaluar, Orientar y Supervisar	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno.	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S	
	EDM02	Asegurar la Entrega de Beneficios	P		S		P	P	P	S			S	S	S	S		S		P
	EDM03	Asegurar la Optimización del Riesgo	S	S	S	P		P	S	S		P			S	S	P	S		S
	EDM04	Asegurar la Optimización de los Recursos	S		S	S	S	S	S	S	P		P		S			P		S
	EDM05	Asegurar la Transparencia hacia las partes interesadas	S	S	P			P	P						S	S	S			S
Alinear, Planificar y Organizar	APO01	Gestionar el Marco de Gestión de TI	P	P	S	S			S		P	S	P	S	S	S	P	P		P
	APO02	Gestionar la Estratégia	P		S	S	S		P	S	S		S	S	S	S	S	S		P
	APO03	Gestionar la Arquitectura Empresarial	P		S	S	S	S	S	S	P	S	P	S		S				S
	APO04	Gestionar la Innovación	S			S	P			P	P		P	S		S				P
	APO05	Gestionar el Portafolio	P		S	S	P	S	S	S	S		S		P					S
	APO06	Gestionar el Presupuesto y los Costes	S		S	S	P	P	S	S			S		S					
	APO07	Gestionar los Recursos Humanos	P	S	S	S			S		S	S	P		P		S	P		P
	APO08	Gestionar las Relaciones	P		S	S	S	S	P	S			S	P	S		S	S		P
	APO09	Gestionar los Acuerdos de Servicio	S			S	S	S	P	S	S	S	S		S	P	S			
	APO10	Gestionar los Proveedores		S		P	S	S	P	S	P	S	S		S	S	S			S
	APO11	Gestionar los Calidad	S	S		S	P		P	S	S		S		P	S	S	S		S
	APO12	Gestionar el Riesgo		P		P		P	S	S	S	P			P	S	S	S		S
	APO13	Gestionar la Seguridad		P		P		P	S	S		P				P				
Construcción, Adquisición e Implementación	BAI01	Gestionar los Programas y Proyectos	P		S	P	P	S	S	S			S		P				S	S
	BAI02	Gestionar la Definición de Requisitos	P	S	S	S	S		P	S	S	S	S	P	S	S				S
	BAI03	Gestionar la Identificació y Construcción de Soluciones	S			S	S		P	S			S	S	S	S				S
	BAI04	Gestionar la Disponibilidad y la Capacidad				S	S		P	S	S		P		S	P				S
	BAI05	Gestionar la Introducción de Cambios Organizativos	S		S		S		S	P	S		S	S	P					P
	BAI06	Gestionar los Cambios			S	P	S		P	S	S	P	S	S	S	S	S			S
	BAI07	Gestionar la Aceptación del Cambio y de la Transición				S	S		S	P	S			P	S	S	S			S
	BAI08	Gestionar el Conocimiento	S				S		S	S	P	S	S			S			S	P
	BAI09	Gestionar los Activos		S		S		P	S		S	S	P			S	S			
	BAI10	Gestionar la Configuración		P		S		S		S	S	S	P			P	S			
Entregar, Dar Servicio y Soporte	DSS01	Gestionar las Operaciones		S		P	S		P	S	S	S	P			S	S	S	S	S
	DSS02	Gestionar las Peticiones e Incidentes del Servicio				P			P	S		S				S	S			S
	DSS03	Gestionar los Problemas		S		P	S		P	S	S		P	S		P	S			S
	DSS04	Gestionar la Comunidad	S	S		P	S		P	S	S	S	S	S		P	S	S	S	S
	DSS05	Gestionar los Servicios de Seguridad	S	P		P			S	S		P	S	S		S	S			
	DSS06	Gestionar los Controles de los Procesos del Negocio		S		P			P	S		S	S	S		S	S	S	S	S
Supervisar, Evaluación y Verificación	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S		S
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno		P		P		S	S	S		S				S	P			S
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos		P		P	S		S			S					S			S

Figura 34 Identificación de Procesos OE1
Fuente: (ISACA, 2012)

Daisy Fernanda Alvarado Carpio
Laura Alexandra Zumba Morales

Con las dos metas de TI identificadas se realiza el correspondiente mapeo para identificar los *PROCESOS* que son necesarios llevar a cabo en la entidad, con el objeto de cumplir con el objetivo de FORTALECER LA ESTRUCTURA ORGANIZACIONAL.

Se debe ubicar en el área de las metas de TI la meta N° 8 al seguir de forma descendente ubicamos solamente los *PROCESOS* primarios, de acuerdo a los dominios tenemos:

- Alinear, Planificar y Organizar se identifica **APO 04**: Gestionar la innovación.
- Construcción, Adquisición e Implementación se identifican dos procesos: **BAI 05**: Gestionar la introducción de cambios organizativos y la **BAI 07**: Gestionar la aceptación del cambio y de la transición.

De igual manera se realiza con la meta N° 16 identificada, que se relaciona según los dominios con:

- Evaluar, Orientar y Supervisar **EDM 04**: Asegurar la optimización de recursos.
- Alinear, Planificar y Organizar **APO 01**: Gestionar el Marco de Gestión de TI y **APO 07**: Gestionar los Recursos Humanos.

Cabe recalcar que los siguientes tres objetivos siguen el mismo procedimiento a fin de determinar todos los procesos que ayuden al cumplimiento de las metas de TI y que posteriormente serán priorizados, para obtener una lista depurada, la cual servirá de base para la fase de análisis de riesgo respecto de los objetivos de la DTIC.

Para resumir los pasos anteriormente desarrollados y con objeto de brindar un medio que permita rápidamente identificar los procesos dentro de un objetivo, se ha considerado la elaboración del siguiente bosquejo:

OE – DTIC	META CORP	META TI	PROCESOS					
FORTALECER LA ESTRUCTURA ORGANIZACIONAL	14	8	APO 04					
			BAI 05	BAI 07				
		16	EDM 04					
			APO 01	APO 07				
AUTOMATIZAR LOS PROCESOS DE LA UNIVERSIDAD	11	1	EDM 01	EDM 02				
			APO 01	APO 02	APO 03	APO 05	APO 07	APO 08
			BAI 01	BAI 02				
		7	EDM 01	EDM 02	EDM 05			
			APO 02	APO 08	APO 09	APO 10	APO 11	
			BAI 02	BAI 03	BAI 04	BAI 06		
			DSS 01	DSS 02	DSS 03	DSS 04	DSS 06	
			MEA 01					
		8	APO 04					
			BAI 05	BAI 07				
		9	EDM 04					
			APO 01	APO 03	APO 04	APO 10		
			BAI 08					
		12	APO 08					
			BAI 02	BAI 07				
	12	5	EDM 02					
			APO 04	APO 05	APO 06	APO 11		
			BAI 01					
		6	EDM 02	EDM 03	EDM 05			
			APO 06	APO 12	APO 13			
			BAI 09					
		11	EDM 04					
			APO 01	APO 03	APO 04	APO 07		
			BAI 04	BAI 09	BAI 10			
			DSS 01	DSS 03				
			MEA 01					
	14	8	APO 04					
			BAI 05	BAI 07				
		16	EDM 04					
			APO 01	APO 07				
MEJORAR PROGRESIVAMENTE LA PRESTACIÓN DE SERVICIOS INFORMÁTICOS	6	1	EDM 01	EDM 02				
			APO 01	APO 02	APO 03	APO 05	APO 07	APO 08
			BAI 01	BAI 02				
		7	EDM 01	EDM 02	EDM 05			
			APO 02	APO 08	APO 09	APO 10	APO 11	
			BAI 02	BAI 03	BAI 04	BAI 06		
			DSS 01	DSS 02	DSS 03	DSS 04	DSS 06	
			MEA 01					
	7	4	EDM 03					

Daisy Fernanda Alvarado Carpio
Laura Alexandra Zumba Morales

			APO 10	APO 12	APO 13			
			BAI 01	BAI 06				
			DSS 01	DSS 02	DSS 03	DSS 04	DSS 05	DSS 06
			MEA 01	MEA 02	MEA 03			
		10	EDM 03					
			APO 12	APO 13				
			BAI 06					
			DSS 05					
		14	APO 09	APO 13				
			BAI 04	BAI 10				
			DSS 03	DSS 04				
MEJORAR DE LA INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	8	1	EDM 01	EDM 02				
			APO 01	APO 02	APO 03	APO 05	APO 07	APO 08
			BAI 01	BAI 02				
		7	EDM 01	EDM 02	EDM 05			
			APO 02	APO 08	APO 09	APO 10	APO 11	
			BAI 02	BAI 03	BAI 04	BAI 06		
			DSS 01	DSS 02	DSS 03	DSS 04	DSS 06	
			MEA 01					
		9	EDM 04					
			APO 01	APO 03	APO 04	APO 10		
			BAI 08					
		17	EDM 02					
			APO 01	APO 02	APO 04	APO 07	APO 08	
			BAI 05	BAI 08				
	9	1	EDM 01	EDM 02				
			APO 01	APO 02	APO 03	APO 05	APO 07	APO 08
			BAI 01	BAI 02				
		14	APO 09	APO 13				
			BAI 04	BAI 10				
			DSS 03	DSS 04				
	10	4	EDM 03					
			APO 10	APO 12	APO 13			
			BAI 01	BAI 06				
			DSS 01	DSS 02	DSS 03	DSS 04	DSS 05	DSS 06
			MEA 01	MEA 02	MEA 03			
		6	EDM 02	EDM 03	EDM 05			
			APO 06	APO 12	APO 13			
			BAI 09					
		11	EDM 04					
			APO 01	APO 03	APO 04	APO 07		
			BAI 04	BAI 09	BAI 10			
			DSS 01	DSS 03				
			MEA 01					
	15	2	APO 01	APO 12	APO 13			

Daisy Fernanda Alvarado Carpio
Laura Alexandra Zumba Morales

			BAI 10					
			DSS 05					
			MEA 02	MEA 03				
		10	EDM 03					
			APO 12	APO 13				
			BAI 06					
			DSS 05					
		15	EDM 03					
			APO 01					
			MEA 01	MEA 02				

Figura 35 Resumen por objetivos
Fuente: Autoras

4.1.2.6. Priorización de procesos por dominios

La priorización se basa en la extracción de los procesos que presentaron una mayor contribución a la consecución de los objetivos, los mismos que servirán posteriormente para: la identificación de prácticas claves de gobierno y determinación de riesgos. Aplicando el conteo de procesos, los priorizados fueron:

CONTEO		DENOMINACIÓN
Evaluar, orientar y supervisar	EDM 01	Asegurar el establecimiento y mantenimiento del marco de gobierno
	EDM 02	Asegurar la entrega de beneficios
	EDM 03	Asegurar la optimización del gobierno
	EDM 04	Asegurar la optimización de recursos
	EDM 05	Asegurar la transparencia hacia las partes interesadas
Alinear, Planificar y Organizar	**APO 01**	Gestionar el marco de gestión de TI
	APO 02	Gestionar la estrategia
	APO 03	Gestionar la arquitectura empresarial
	APO 04	Gestionar la innovación
	APO 05	Gestionar el portafolio
	APO 06	Gestionar el presupuesto de costes
	APO 07	Gestionar los recursos humanos
	APO 08	Gestionar las relaciones
	APO 09	Gestionar los acuerdos de servicios
	APO 10	Gestionar los Proveedores
	APO 11	Gestionar la calidad
	APO 12	Gestionar el riesgo
	APO 13	Gestionar la seguridad
Construcción, Adquisición e Implementación	**BAI 01**	Gestionar los programas y proyectos
	BAI 02	Gestionar la definición de requisitos
	BAI 03	Gestionar la identificación y construcción de soluciones
	BAI 04	Gestionar la disponibilidad y capacidad
	BAI 05	Gestionar la introducción del cambio organizativo
	BAI 06	Gestionar los cambios
	BAI 07	Gestionar la aceptación del cambio y la transición
	BAI 08	Gestionar el conocimiento

a 36 Priorización de Procesos
Fuente: (ISACA, 2012)

	BAI 09	Gestionar los activos
	BAI 10	Gestionar la configuración
Entregar, Dar servicio y Soporte	**DSS 01**	Gestionar las operaciones
	DSS 02	Gestionar peticiones e incidentes de servicio
	DSS 03	Gestionar los problemas
	DSS 04	Gestionar la continuidad
	DSS 05	Gestionar los servicios de seguridad
	DSS 06	Gestionar controles de procesos de negocio
Supervisión, Evaluación y Verificación	**MEA 01**	Supervisar, Evaluar y Valorar rendimiento y conformidad.
	MEA 02	Supervisar, Evaluar y Valorar el sistema de control interno
	MEA 03	Supervisar, evaluar y valorar la conformidad con los requisitos externos.

OBJETIVOS	PROCESOS																	
	EDM		APO					BAI				DSS					MEA	
	02	04	01	04	07	08	13	01	02	04	06	01	03	04	05	01	02
FORTALECER LA ESTRUCTURA ORGANIZACIONAL		X	X	X	X												
AUTOMATIZAR LOS PROCESOS DE LA UNVERSIDAD	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		
MEJORAR PROGRESIVAMENTE LA PRESTACIÓN DE SERVICIOS INFORMÁTICOS	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		
MEJORAR DE LA INFRAESTRUCTURA DE TIC	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Figura 37 Resumen de Priorización por Objetivos
Fuente: (ISACA, 2012)

El aporte que pretende el dominio EDM (Evaluar, Orientar y Sustentar), está encaminado únicamente a la parte de gobierno que es de responsabilidad del Consejo Administrativo, por lo que nuestro análisis se enfocará en establecer una metodología de gestión de riesgo para lo cual tiene alta significatividad los restantes cuatro dominios que se enfocan en la gestión, pero de manera especial considerando el proceso APO 12 que hace referencia al planteamiento, ejecución, control y evaluación de las actividades que permiten el tratamiento del riesgo lo cual responde al cumplimiento de los objetivos de la tesis.

Los riesgos se presentan en las actividades relacionadas a la gestión por lo cual se vuelve primordial su análisis para la identificación y respuesta oportuna a los riesgos.

4.1.2.7. Identificación de las prácticas claves de gobierno que apoyan al cumplimiento de los objetivos de TI o la normativa de Control Interno

Definidas previamente las metas corporativas se deben analizar las prácticas claves de gobierno que se detallan en *COBIT 5 Procesos Catalizadores,* según las actividades y el objetivo de cada una de estas se puede identificar cuál de

ellas pueden aportar al cumplimiento de las metas con su implementación así como con la normativa.

Se debe mencionar que respecto de las metas los procesos que se analizan únicamente son los priorizados mientras que para el cumplimiento de la normativa se analizan todos los procesos que presenta *COBIT 5 Procesos Catalizadores* exceptuando el dominio EDM.

Ejemplo:

Objetivo N°1: Fortalecer la estructura organizacional de la DTIC

DENOMINACIÓN	PROCESOS	PRÁCTICA CLAVE DE GOBIERNO		1.Fortalecer la estructura organizacional
ALINEAR, PLANIFICAR Y ORGANIZAR	**APO 01** Gestionar el marco de gestión de TI	**.01**	Definir la estructura organizativa	
		.02	Establecer roles y responsabilidades	
		.03	Mantener los elementos catalizadores del sistema de gestión	■
		.04	Comunicar los objetivos y la dirección de gestión	
		.05	Optimizar la ubicación de la función de TI	
		.06	Definir la propiedad de la información (datos) del sistema	
		.07	Gestionar la mejora continua de los procesos	■
		.08	Mantener el cumplimiento con las políticas y procedimientos	
	APO 02 Gestionar la Estrategia	**.01**	Comprender la dirección de la empresa	
		.02	Evaluar el entorno, capacidades y rendimientos actuales	
		.03	Definir el objetivo de las capacidades de TI	
		.04	Realizar un análisis de diferencias	
		.05	Definir el Plan Estratégico y la hoja de ruta	
		.06	Comunicar la estrategia y la dirección de TI	
	APO 03 Gestionar la Arquitectura Empresarial	**.01**	Desarrollar la visión de la arquitectura de la empresa	
		.02	Definir la arquitectura de referencia	
		.03	Seleccionar las oportunidades y las soluciones	
		.04	Definir la implantación de la arquitectura	
		.05	Proveer los servicios de arquitectura empresarial	
	APO 04 Gestionar la innovación	**.01**	Crear un entorno favorable para la innovación	■
		.02	Mantener un entendimiento del entorno de la empresa	
		.03	Supervisar y explorar el entorno tecnológico	
		.04	Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras	
		.05	Recomendar iniciativas apropiadas adicionales	
		.06	Supervisar la implementación y el uso de la innovación	
	APO 05 Gestionar el Portafolio	**.01**	Establecer la meta del objetivo de inversión	
		.02	Determinar la disponibilidad y las fuentes de fondos	
		.03	Evaluar y seleccionar los programas	
		.04	Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones	
		.05	Mantener los portafolios	
		.06	Gestionar la consecución de beneficios	
	APO 06 Gestionar el Presupuesto y los Costes	**.01**	Gestionar la finanzas y la contabilidad	
		.02	Priorizar la asignación de recursos	
		.03	Crear y mantener presupuestos	
		.04	Modelar y asignar costes	
		.05	Gestionar costes	
	APO 07 Gestionar los recursos humanos	**.01**	Mantener la dotación de personal suficiente y adecuado	
		.02	Identificar personal clave de TI	
		.03	Mantener las habilidades y competencias del personal	■
		.04	Evaluar el desempeño laboral de los empleados	
		.05	Planificar y realizar un seguimiento del uso de los recursos humanos de TI y del negocio	
		.06	Gestionar el personal contratado	
	APO 08 Gestionar las relaciones	**.01**	Entender las expectativas del negocio	
		.02	Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio	
		.03	Gestionar las relaciones con el negocio	
		.04	Coordinar y comunicar	
		.05	Proveer datos de entrada para la mejora continua de los servicios	

Figura 38 Identificación de prácticas para lograr los objetivos de la DTIC
Fuente: Autoras

Para el objetivo *FORTALECER LA ESTRUCTURA ORGANIZACIONAL* cuya meta corporativa se identificó como *productividad operacional y de los empleados* con sus respectivas metas de TI priorizadas, se obtiene un total de

tres procesos priorizados de los catorce (excluyendo los procesos EDM) que se presentaron:

- **APO01**: Gestionar el Marco de Gestión de TI
- **APO04**: Gestionar la Innovación
- **APO07**: Gestionar los Recursos Humanos (siendo el más importante.)

Recordando que el objetivo se centra en brindar la capacitación idónea al personal de TI así como el establecimiento de metodologías para el desarrollo, mantenimiento e implementación de software y estructuras del departamento.

De las prácticas que tiene cada proceso, en este caso ocho y seis, se analiza cuidadosamente cada una teniendo en cuenta entradas, salidas y actividades para definir cual se acopla a las necesidades institucionales.

Para APO 01 Gestionar el marco de Gestión de TI, se determinan las siguientes:

03. Mantener los elementos catalizadores del sistema de gestión.- Permite mantener el entorno de gestión y control así como alinear estos al estilo y filosofía de la empresa e inclusive con mejores prácticas reconocidas globalmente. De este resultan las políticas relacionadas con TI y todo el proceso relacionado.

04. *Comunicar los objetivos y la dirección de gestión.*- Esta favorece a la comunicación y comprensión de objetivos de TI por parte de las partes relacionadas, proceso fundamental para fortalecer la estructura organización y permite el desarrollo de acciones en pro de un beneficio.

07. *Gestionar la mejora continua de los procesos.*- Se relaciona directamente con el fortalecimiento e implica la evaluación, planificación y ejecución de mejora continua de los procesos además contempla la actualización. Las salidas incluyen oportunidades e indicadores.

08. *Mantener el cumplimiento con las políticas y procedimientos.*- Implica la puesta en práctica de las políticas y actualizaciones aprobadas de las mismas.

Las actividades se encaminan al seguimiento y adopción de medidas correctivas para eventos determinados de incumplimiento.

En el caso de APO 04: Gestionar la Innovación se seleccionó la siguiente práctica:

01. *Crear un entorno favorable para la innovación*.- Ya que apoya a la entidad para que tome en consideración las ideas de los empleados y demás colaboradores en pro de la mejora institucional a través de la innovación, lo cual fortalece a la misma, ello a través de la generación de un plan de innovación así como aplicación de incentivos.

Y finalmente para el ejemplo indicado para APO 07: Gestionar los Recursos Humanos se determinó las siguientes:

03. *Mantener las habilidades y competencias del personal*.- Representa un punto clave para la institución la preparación del personal en el desarrollo de sus actividades, implementando tecnologías que faciliten y mejoren su desempeño, lo que implica necesidades de actualizaciones para el mismo.

04. *Evaluar el desempeño laboral de los empleados*.- Apoya a la medición del cumplimiento de las expectativas que se espera de sus empleados.

05. *Planificar y realizar un seguimiento del uso de los recursos humanos de TI y del negocio*.- El conocimiento respecto a cómo se manejan los recursos es básico para la entidad permitiéndole optimizar los mismos y asegurar que son utilizados para los fines inicialmente planteados.

Como actividades importantes están los inventarios, análisis de deficiencias e información referente. De la misma manera se procede con todos los procesos priorizados.

En el caso de la priorización de prácticas que permitan el cumplimiento de ***la normativa de Control Interno de la Contraloría General del Estado***, se analizaron todas las prácticas de los cuatro dominios relacionados con gestión

de acuerdo a los requerimientos detallados en la misma, independientemente de si el proceso está o no priorizado.

La normativa base se encuentra dentro del componente *ACTIVIDADES DE CONTROL* el subgrupo *410: Tecnologías de la información*, mismo que se encuentra subdivida en diecisiete normas relacionadas como son:

- *410-01 Organización Informática*
- *410-02 Segregación de Funciones*
- *410-03 Plan Informático Estratégico de Tecnología*
- *410-04 Políticas y procedimientos*
- *410-05 Modelo de formación organizacional*
- *410-06 Administración de Proyectos Tecnológicos*
- *410-07 Desarrollo y Adquisición de Software Aplicativo*
- *410-08 Adquisiciones de infraestructura tecnológica*
- *410-09 Mantenimiento y Control de la Infraestructura Tecnológica*
- *410-10 Seguridad de la TI*
- *410-11 Plan de Contingencias*
- *410-12 Administración de Soporte de TI*
- *410-13 Monitoreo y Evaluación de Procesos y Servicios*
- *410-14 Sitio web, servicio de internet e intranet*
- *410-15 Capacitación Informática*
- *410-16 Comité informático*
- *410-17 Firmas Electrónicas* (Contraloría General del Estado, 2009)

Ejemplo:

Norma 410-01: Organización Informática

PROCESOS	PRÁCTICA CLAVE DE GOBIERNO	NORMATIVA																
		Organización Informática	Segregación de Funciones	Plan informático Estratégico de tecnología	Políticas y procedimientos	Modelo de formación organizacional	Administración de proyectos tecnológicos	Desarrollo y adquisición de software aplicativo	Adquisiciones de infraestructura tecnológica	Mantenimiento y control de la infraestructura tecnológica	Seguridad de la TI	Plan de contingencias	Administración de Soporte de TI	Monitoreo y evaluación de procesos y servicios	Sitio web, servicio de internet e intranet	Capacitación Informática	Comité informático	Firmas
APO 01 Gestionar el marco de gestión de TI	.01 Definir la estructura organizativa	■															■	
	.02 Establecer roles y responsabilidades		■															
	.03 Mantener los elementos catalizadores del sistema de gestión				■										■			
	.04 Comunicar los objetivos y la dirección de gestión																	
	.05 Optimizar la ubicación de la función de TI	■																
	.06 Definir la propiedad de la información (datos) del sistema					■												
	.07 Gestionar la mejora continua de los procesos																	
	.08 Mantener el cumplimiento con las políticas y procedimientos				■													

Figura 39 Identificación de prácticas para el cumplimiento de la normativa
Fuente: Autoras

Para la norma, definen prácticas que permitan posesionar al área de TI *como unidad de apoyo y asesoría* para la dirección, lo que implica que la entidad debe trabajar conjuntamente y en crecimiento con las TI, considerando que estas permiten agregar valor a las actividades y generar ventajas a nivel externo, para ello requiere la colaboración de las partes relacionadas sin caer en la dependencia y asegurando el monitoreo continuo.

Con el entendimiento de los requerimientos se revisaron las actividades de los procesos así como las salidas, para identificar las siguientes prácticas:

PRÁCTICA	ACTIVIDADES	SALIDAS
APO01.01	Las actividades apoyan a la participación de las partes interesadas lo que beneficia a la transparencia, la definición de estructuras y relaciones de gestión que favorecen el control. Así también colabora con la revisión permanente para asegurar la adecuación de la misma, ajustando estrategias internas y demás particulares.	Roles y responsabilidades asignadas a la personas dentro de TI. Prácticas para llevar a cabo la supervisión
APO01.05	Comprender y entender la importancia del área de TI dentro de la estructura organizativa global, lo cual requerirá la aprobación de sus funciones reconociendo de este modo la importancia que tiene esta área dentro de la organización.	Opciones para la ubicación del área de TI. Detalle de las funciones del área de TI.

Figura 40 Salidas de APO 01 y sus prácticas
Fuente: Autoras

El proceso detallado anteriormente se aplica de igual manera para toda la normativa.

A través del análisis efectuado en este primer paso, se ha logrado un entendimiento general sobre el ámbito de riesgos y se han establecido aquellos procesos prioritarios que aportan al cumplimiento de la normativa vigente de Control Interno así como de los objetivos institucionales, lo cual sirve como una entrada de información para el siguiente paso que será la obtención de escenarios de riesgos y análisis de estos. Ver ANEXO 4.

4.2. Analizar el Riesgo

4.2.1. Identificación de escenarios

De acuerdo con el procedimiento planteado en el capítulo anterior, en este apartado se considera iniciar con la identificación de aquellos escenarios de riesgos propuestos en la plantilla provista por COBIT 5 *para Riesgos* aplicables en el desarrollo del presente trabajo.

En este caso sólo se los ha tomado como referencia para entender cómo se debe estructurar el escenario, debido a la interacción que se pretende entre objetivos y normativa. Ver ANEXO 5. Puesto que anteriormente se aplicó la priorización de procesos la generación de los escenarios de riesgo será directa, es decir, no se elaborarán dos listados de riesgos que luego se combinen en un listado final.

Los riesgos han sido identificados únicamente para los procesos priorizados dentro de los cuales se identifican prácticas que aportan al cumplimiento normativo así como institucional por lo cual requieren un tratamiento prioritario. Cabe mencionar también, que no se pueden adoptar una sola práctica dentro de un proceso por ello se identifican riesgos relacionados con las demás prácticas del proceso.

La formulación de los escenarios de riesgos se basa en la estructura de los escenarios de riesgos proporcionados por *COBIT 5 para Riesgos,* el cual

presenta veinte situaciones en las cuales una entidad en general puede sufrir pérdidas, sin embargo, como se mencionó en la parte teórica estos riesgos deben ser comparados con la realidad de la entidad de manera que el resultado sea objetivo y pertinente.

De las categorías presentadas la denominada *Geopolítica* se excluye del análisis ya que en el país las condiciones políticas no representan ser limitantes, debido a que se motiva a la búsqueda de la automatización de los servicios prestados por las entidades en favor de incrementar la eficiencia y eficacia siempre enfocados en el bienestar de los usuarios.

La categoría denominada *Staff Operacional* se ha acoplado a otras categorías relacionadas con hardware y software, debido a que se contemplan riesgos generados con estos a raíz de errores del personal o intentos maliciosos, por lo cual no se lo identifica explícitamente.

Únicamente se han considerado los escenarios negativos los cuales se encuentran relacionados con los procesos que se necesitan para dar cumplimiento normativo y apoyo a la estrategia, pero también pueden formularse escenarios positivos que están direccionados a las oportunidades.

Finalmente, cada uno de los riesgos se ha considerado según su efecto, como **P**rimarios o **S**ecundarios, recurriendo a las tres tipos de riesgo definidos:

- Beneficio de TI /Habilitador de valor
- Programa de TI o proyecto entregado
- Operaciones de servicios de TI entregados

El escenario de Riesgos completos para la Dirección de Tecnologías y Comunicación de la Universidad de Cuenca se puede apreciar en el ANEXO 6.

Ejemplo:

Para explicar la formulación de los escenarios, se procede a tomar la primera de las dieciocho categorías elegidas, de la plantilla de *COBIT 5 para Riesgos*.

Categoría N°1: Establecimiento y Mantenimiento del Portafolio

CATEGORIA DEL ESCENARIO DE RIESGO	Tipo de Riesgo			N°	ESCENARIOS NEGATIVOS	P
	Beneficio de TI/ Habilitación de valor	Programa de TI y proyecto entregado	Operaciones de Servicios de TI			
Establecimiento y mantenimiento del portafolio	P	S	S	1	Desactualización de las políticas de TI.	
	P	S	P	2	Escasez o descoordinación de requerimientos de control con relación a los objetivos o su inoportuna ejecución.	
	P	S	S	3	No existe correlación entre los objetivos del negocio y TI. (Alineación Estratégica)	
		P	S	4	Desconocimiento de los objetivos y metas institucionales que imposibilitan el posterior análisis sobre su rendimiento.	
	P	S	S	5	Falta de seguimiento y control de las soluciones implementadas.	
	P	S	S	6	Rezagar al área de TI dentro de la estructura organizacional, sin considerar su importancia y criticidad para la consecución de objetivos.	
	S	S	P	7	Las partes interesadas no son participantes activas para la entidad.	
	S	P	S	8	Requerimientos no comunicados ni aprobados antes de su puesta en marcha.	

Figura 41 Escenario de Riesgos
Fuente: (ISACA, 2012) - Autoras

Para la primera categoría se ha determinado un total de ocho riesgos de los cuales todos implican incumplimiento tanto de la normativa así como de los objetivos de la entidad (aquellos señalados de color). A ésta definición se llegó de la siguiente manera:

a. Desactualización de las políticas de TI

La entidad para poder manejar adecuadamente las TI define políticas respecto de: seguridad, conectividad, internet, activos, etc., sin embargo, estas políticas deben actualizarse de manera permanente ya que el entorno es cambiante, especialmente en el área tecnológica donde la seguridad de la información así como la propia infraestructura requieren de atención continua.

Por ejemplo, respecto de la seguridad, la configuración de firewalls así como la revisión de actividad de virus se vuelve crítica pues día a día se generan nuevas versiones que se vuelven más discretas y afectan a mayores proporciones de un sistema, por ello la política que se direccione a las seguridad debe ser clara y flexible, pero adicionalmente se deben definir los suficientes procedimientos para materializar la misma e ir actualizando todo de manera regular conforme lo exige el crecimiento tecnológico.

Si la entidad no tiene políticas actualizadas de TI limitaría el logro del OE N°1 enfocado en fortalecer la estructura de la entidad, pues políticas, procedimientos y estándares conforman la base de una adecuada estructura.

Adicionalmente, se incumpliría la normativa referente a políticas, procesos y estándares que dice: *estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran.* (Contraloría General del Estado, 2009).

Por lo mencionado se considera el riesgo como **Primario** en lo referente a la habilitación de valor pues la efectividad de un proceso que se basa en el uso de la tecnología se ve comprometida por no estar actualizadas las políticas y sus correspondientes políticas.

b. Escasez o descoordinación de requerimientos de control con relación a los objetivos o su inoportuna ejecución

El control respecto del cumplimento de los objetivos, es indispensable para poder tomar los correctivos necesarios en los proyectos, programas o actividades que estén siendo llevados a cabo o al contrario no se encuentren planeados. La ausencia de control ocasiona que los recursos estén erróneamente utilizados y los objetivos no se cumplan de manera satisfactoria ya que las desviaciones no se detectan o se lo hace tardíamente también cabe

la posibilidad de que el control sea ineficiente por no brindar la información suficiente.

Este riesgo interfiere con la consecución de los cuatros OE y adicionalmente se contrapone a lo que establece la normativa respecto de los planes estratégicos que se manejan, en ésta se establece que *se actualizarán de manera permanente, además de ser monitoreados y evaluados en forma trimestral para determinar su grado de ejecución y tomar las medidas necesarias en caso de desviaciones.* (Contraloría General del Estado, 2009)

Para el tipo de riesgo se han considerado como Primario a dos de ellos: Habilitación de valor y Operaciones de Servicios de TI entregados pues el riesgo afecta la operatividad de la entidad y genera destrucción del valor por la ausencia o ineficiencia del control.

c. No existe correlación entre los objetivos del negocio y TI. (Alineación Estratégica)

La correlación de los objetivos de la DTIC y la institución es indispensable de manera que los esfuerzos se direccionen a un mismo horizonte. La alineación estratégica es resaltada ya que constituye la base de *COBIT 5.*

Al no existir correlación la entidad no podrá cumplir sus objetivos porque la DTIC no brindará apoyo para lograrlos, al contrario, puede convertirse en un freno ocasionando destrucción de valor.

El riesgo afecta a todos los OE y se contrapone al cumplimento de lo presentado en la normativa *el plan informático estratégico tendrá un nivel de detalle suficiente para permitir la definición de planes operativos de tecnología de Información y especificará como ésta contribuirá a los objetivos estratégicos de la organización.* (Contraloría General del Estado, 2009)

El riesgo es considerado como **Primario** en relación a la capacidad de TI para generar valor agregado para la entidad, pues la correlación entre TI y la entidad en general ayuda a direccionar proyectos y optimizar recursos.

d. Desconocimiento de los objetivos y metas institucionales que imposibilitan el posterior análisis sobre su rendimiento.

Lo que no se conoce no se puede administrar o gestionar, esto aplica a cabalidad en la ejecución de todos los OE pero afecta directamente al OE N°2, puede que las propuestas sean muy buenas pero que no aporten o se relacionen directamente con la automatización de los procesos, en esto se pierde: tiempo, recursos monetarios y otros; todo debido a que los objetivos no son conocidos y entendidos por las personas de la organización encargas de la planeación.

Respecto de la normativa ésta establece que *será necesario establecer procedimientos de comunicación, difusión y coordinación entre las funciones de tecnología de información y las funciones propias de la organización.* (Contraloría General del Estado, 2009)

El riesgo califica como **Primario** para Programas y Proyectos de TI entregados pues al momento de formular una solución ésta debe estar conforme a los objetivos que se persiguen institucionalmente y a nivel de la DTIC pues constituye la base para seguir el correspondiente ciclo de vida por lo que sí es erróneo todo el proyecto falla.

e. Falta de seguimiento y control de las soluciones implementadas.

Con la implementación de la solución no termina el ciclo de vida del programa proyecto, pues es necesario que se dé un seguimiento y control adecuado estableciendo para ello medidas, responsables y otros.

Si no se controla entonces no se podrá detectar lo que el usuario necesita como: cambios, sugerencias o desconformidades por ende no se cumple con el fin por el cual la solución fue implementada. El riesgo se relaciona con el OE N°2.

En relación a la normativa se establece que *se cubrirá, como mínimo las etapas de: inicio, planeación, ejecución, control, monitoreo y cierre de proyectos* y en otra parte *es necesario establecer un marco de trabajo de monitoreo y definir el alcance, la metodología y el proceso a seguir para monitorear la contribución*

y el impacto de tecnología de información en la entidad. (Contraloría General del Estado, 2009)

El riesgo se califica como **Primario** respecto de la Habilitación de Valor pues toda solución implementada debe ser supervisada con el objetivo de verificar si cumple con las necesidades del usuario, posibles mejoras o nuevos requerimientos.

f. Rezagar al área de TI dentro de la estructura organizacional, sin considerar su importancia y criticidad para la consecución de objetivos.

Como se resalta la TI puede brindar una ventaja competitiva si ésta es correctamente administrada por lo cual si la entidad rezaga al área de TI sin considerar su importancia y criticidad entonces dicha ventaja no se logrará. Además, dentro de la institución todas las unidades de negocio son importantes, con aportes dentro del área que les compete y por ello deben considerarse en la consecución de objetivos.

El objetivo que se ve afectado es el OE N°1 y respecto de la normativa se incumple lo establecido *la unidad de tecnología de información, estará posicionada dentro de la estructura organizacional de la entidad en un nivel que le permita efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias; así como participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica. Además debe garantizar su independencia respecto de las áreas usuarias y asegurar la cobertura de servicios a todas las unidades de la entidad u organismo.* (Contraloría General del Estado, 2009)

Respecto de este riesgo se califica como **Primario** para la habilitación de valor, pues su efecto se centra en dejar a la DTIC aislada y no considerar su aporte a la entidad, por medio de los proyectos tecnológicos, a ser una universidad automatizada conforme las exigencias de la globalización y a nivel de las universidades del denominado primer mundo.

g. Las partes interesadas no son participantes activas para la entidad.

El mantenimiento de un entendimiento del entorno de la empresa influencia de manera trascendental en la coordinación y comunicación efectuada con las diversas partes interesadas debido a que el trabajo efectuado no es individual sino más bien se fomenta al trabajo en equipo, razón por la cual dichos aspectos deben ser considerados por la DTIC ya que presenta falencias en la coordinación con partes interesadas tanto en el planteamiento como aprobación del Plan Operativo Anual entre otros planes, debido a la ausencia de la programación de reuniones entre ellas y las unidades del negocio además imposibilita conocer posibles mejoras o simplemente coordinar sus las necesidades globales en aspectos emergentes o habituales.

Este riesgo afecta al OE N° 2 puesto que para este se requiere la consideración de las partes interesadas dentro de la institución con el fin de solventar las necesidades de las mismas, y a la vez, saber lo que los usuarios externos realmente necesitan o esperan de la DTIC y sus servicios.

En relación a la normativa se genera incumplimiento con respecto a que *se establecerá un plan de control de cambios y un plan de aseguramiento de calidad que será aprobado por las partes interesadas*. (Contraloría General del Estado, 2009)

Para este riesgo se ha evaluado que de los tres tipos de riesgos afecta a Operaciones de Servicios de TI Entregados considerado como **Primario**, esto porque la falta de atención a aquellas partes implica un determinado nivel de problemas respecto de los entregables de un programa o proyecto relacionado con TI.

h. Requerimientos no comunicados ni aprobados antes de su puesta en marcha.

Los requerimientos de información de negocio, funcionales, técnicos y de control tienen que ser claros, oportunos, suficientes, concisos, comprensibles y formales con el fin de lograr el alcance de los resultados esperados de las diversas propuestas establecidas caso contrario la entidad incurre en pérdidas

económicas, retrasos y un ambiente de incertidumbre y duda para las personas involucradas.

Es por ello que afecta tanto al OE N° 2 y a la normativa en el tema de desarrollo y adquisición de software aplicativo (Proyecto) en donde se detalla que la *Identificación, priorización, especificación y acuerdos de los requerimientos funcionales y técnicos institucionales con la participación y aprobación formal de las unidades usuarias. Esto incluye, tipos de usuarios, requerimientos de: entrada, definición de interfaces, archivo, procesamiento, salida, control, seguridad, plan de pruebas y trazabilidad o pistas de auditoría de las transacciones en donde aplique.* (Contraloría General del Estado, 2009)

Este riesgo se considera **Primario** para el tipo de riesgo denominado como Programa de TI y proyecto entregado, debido que sus efectos se direccionan al desarrollo de soluciones así como a la ejecución de programas lo cual impide la contribución de TI al negocio.

De los quince procesos priorizados (exceptúan EDM sino serían diez y siete) doce de estos permiten el cumplimiento de la normativa así como la consecución de los objetivos, dejando de lado los procesos: APO13 Gestionar la Seguridad, BAI04 Gestionar la Disponibilidad y Capacidad y finalmente el proceso DSS03 Gestionar los Problemas; pues estos permiten únicamente alcanzar objetivos institucionales.

El procedimiento para definir los escenarios de riesgo es el mismo para los demás procesos y su resultado final será utilizado como una plantilla de la cual se elegirán según corresponda el caso conforme la encuesta, los riesgos reales dentro de la DTIC que posteriormente serán tratados.

4.2.2. Análisis del Riesgo

Hasta este punto se ha descrito *el cómo debería ser* (definición de procesos prioritarios que la entidad debería implementar) pero para poder llegar a una eficiente gestión del riesgo se debe conocer el *cómo es* actualmente el ambiente de riesgos de la DTIC. Por ello, se procedió a la realización de una entrevista

dirigida, basada en los procesos priorizados y la normativa, de manera que los resultados obtenidos posteriormente se mapeen con los escenarios de riesgos anteriormente definidos, lo cual constituye la base para el análisis propio de riesgos y la definición de los niveles correspondientes.

La entrevista se realizó a dos personas que encabezan la DTIC de la Universidad, el director entrante Ing. Patricio Guerrero y la directora saliente de la DTIC la Ing. Carmita Rojas, que según se consideró, tienen un conocimiento integral del área que dirigen y sus respuestas aportan sustancialmente a los fines perseguidos.

La encuesta se dividió en veinte y dos bloques con preguntas abiertas y cerradas dependiendo de la naturaleza y objetivo de las mismas. Las preguntas han sido definidas en un contraste positivo, es decir, si las respuestas son afirmativas las actividades no representarían riesgo caso contrario implicaría un riesgo para la entidad que será tomado en cuenta para la posterior evaluación y calificación. Ver ANEXO 7.

Ejemplo 1:

Para soportar el proceso APO03 en la práctica 07: *Mantener las competencias y habilidades del personal,* así como la norma de CI 410-15: *Capacitación Informática* se ha definido el siguiente objetivo y las preguntas correspondientes que lo soportan.

OBJETIVO: *Conocer si el personal de TIC tiene las competencias necesarias para desempeñar sus actividades y por parte de la organización existe un interés en mantener y mejorar las habilidades del personal a través de planes relacionados y evaluaciones pertinentes.*

PREGUNTAS:

1. Dentro de la DTIC ¿se encuentra definido un método de evaluación al personal enfocado en las habilidades y competencias necesarias para lograr los objetivos

de la empresa, de esta área y procesos en general? ¿En qué consiste dicho método? ¿Con qué probabilidad se lo aplica?

2. ¿Se actualizan periódicamente los planes de acción referentes a: la formación, contratación, redistribución y los cambios en las estrategias de contratación?

3. ¿Se dispone de un Manual de funciones para el personal de TIC?

4. ¿Se dispone de un Plan de Carrera?

5. ¿Se cuenta con un Plan de Capacitación al personal?

6. ¿Se encuentra definido un procedimiento para la sucesión de cargos? ¿Cuál es?

En este caso las respuestas obtenidas no fueron cien por ciento positivas debido a la ausencia de métodos para la evaluación del personal así como procedimientos para la sucesión de cargos.

Ejemplo 2:

Con el fin de cumplir las actividades que se contemplan en el proceso DSS 04: *Gestionar la continuidad* se plantean las siguientes preguntas de manera que con su respuesta se pueda corroborar el cumplimiento de la norma 410-11 *Plan de Contingencias* detallada en el literal número tres. El objetivo y las preguntas correspondientes se definieron de la siguiente manera:

OBJETIVO: *Establecer que la organización ha definido una política de continuidad basada en los objetivos del negocio y los intereses de las partes interesadas.*

PREGUNTAS:

1. ¿Se han identificado procesos de negocio, propios o subcontratados, que sean críticos para las operaciones del negocio?

2. ¿Se maneja un Plan de Continuidad del Negocio?

3. ¿Se encuentran definidas las políticas de continuidad y alcances mínimos de las mismas?

OBJETIVO: *Verificar que la organización supervisa el plan de continuidad con regularidad y aplica la gestión de cambios cuando las circunstancias lo ameriten.*

PREGUNTAS:

1. ¿Se actualiza periódicamente el plan de continuidad acorde a la realidad en la cual la organización desarrolla sus actividades?
2. ¿Se realiza un análisis de riesgos de nuevos cambios acerca de las amenazas potenciales sobre los procesos de negocio y su impacto?

En este caso las respuestas no fueron afirmativas en un cien por ciento ya que la entidad no ha planteado e implementado un Plan de Continuidad para sus operaciones.

Con los resultados de la entrevista se identifican cuáles son los escenarios de riesgo que se relacionan y son más susceptibles de materialización. Ver ANEXO 8.

Ejemplo 1:

Los escenarios de riesgos identificados para el bloque *Mantener las habilidades y competencias del personal* son los siguientes:

OBJETIVO	N° de Riesgo	RIESGO
Conocer si el personal de TIC tiene las competencias necesarias para desempeñar sus actividades y por parte de la organización existe intereses en mantener y mejorar las habilidades del personal a través de planes relacionados y evaluaciones pertinentes.	*43*	Inexistencia de métodos para la evaluación del personal.
	45	Ausencia de planes de desarrollo-mejora de habilidades y competencias del personal de TI lo que provoca brechas en las habilidades que poseen estos respecto a las nuevas tecnologías o métodos. (INTERNO)
	51	No se encuentran claramente definidas las habilidades y competencias necesarias para ocupar un puesto en TI.

Figura 42 Riesgos levantados según encuesta EJ1
Fuente: Autoras

Los escenarios identificados corresponden a los siguientes riesgos listados: Nº 43, 45 y 51 dentro de la categoría de *Experiencia y habilidades en TI.* Estos riesgos surgen de la ausencia de un método para evaluar al personal enfocado en sus habilidades y competencias, lo cual ocasiona que la entidad no tenga conocimiento sobre las falencias que existen en relación al personal por tanto no se idean planes de mejora para ellos y su formación con respecto a nuevas tecnologías o métodos para tratar con TI; el no ser adecuada dicha formación se puede reflejar en fallas o errores en las actividades o procesos relacionados con eficiencia o eficacia.

Para ocupar un puesto dentro de TI, se debería realizar constantemente una evaluación al personal del área así como las necesidades de la institución, que debido a la globalización y avances tecnológicos cambian de manera acelerada lo cual implica que el perfil de un empleado o colaborador del área de TI debe también cambiar, pero en la entidad no se realiza esta actividad lo que significa que existe una constante en las competencias del personal. Como se puede observar la falta de un plan de mejora desencadena varios riesgos para la entidad.

Ejemplo 2:

Para los bloques: *Definir la política de continuidad del negocio, objetivos y alcance* así como *Revisar, mantener y mejorar el plan de continuidad,* se determinan los siguientes riesgos:

OBJETIVO	Nº de Riesgo	RIESGO
Establecer que la organización ha definido una política de continuidad basada en los objetivos del negocio y los intereses de las partes interesadas	*27*	Degradación de la imagen de la entidad por su incapacidad para responder oportuna y asertivamente contra incidentes que afectan a los servicios entregados por proyectos ineficientes.
	68	Falta de un plan de continuidad que imposibilita responder a incidentes e interrupciones de servicios.
	146	Exposición alta a daños por ejecución de malware.

Figura 43 Riesgos levantados según encuesta EJ2
Fuente: Autoras

Como se puede observar se han levantado tres escenarios de riesgos N° 27, 68 y 146 correspondientes al primer objetivo siendo el más relevante el N°68 que expresa la escasez de un Plan de Continuidad, lo cual evidencia que la entidad no posee acciones a seguir en el caso de la presentación de incidentes que afecten la prestación de servicios, ocasionando que las amenazas a las cuales se enfrenta sean más factibles de ocurrencia imposibilitando así el normal funcionamiento de sus actividades y pudiendo desencadenar en la falta de prestigio por no disponer de respuestas inmediatas y oportunas; mientras que para el segundo objetivo que trata sobre la supervisión de las acciones de continuidad este no se puede lograr porque la Universidad no dispone de dicho plan.

El Plan de Continuidad representa una herramienta de apoyo para la entidad es por ello que su planeación, elaboración, aprobación y uso debe ser considerado como fundamental en especial para la DTIC porque es el área más susceptible a eventualidades dañinas tanto internas como externas que pueden afectar al normal desenvolvimiento de las actividades de la entidad relacionadas a procesos, servicios y demás.

Una vez que se han identificado los escenarios de riesgo correspondientes, se procede a la calificación de riesgos en base a probabilidad e impacto. (Ver ANEXO 9). Para ello se ha decidido emplear un método mixto que combine datos cuantitativos con cualitativos, por lo cual para comodidad se ha determinado una tabla de valores para calificar:

PROBABILIDAD		
CALIFICACION	**EXPRESIÒN**	**RELACIÓN**
3	Alto	70-100%
2	Medio	40-70%
1	Bajo	0-40%

Figura 44 Calificaciones para Probabilidad
Fuente: Autoras

IMPACTO		
CALIFICACION	**EXPRESIÒN**	**RELACIÒN**
3	Alto	Cumplimiento normativo y de objetivos estratégicos de la DTIC
2	Medio	Cumplimiento normativo o de objetivos estratégicos de la DTIC
1	Bajo	No afecta a ninguno de ellos

Figura 45 Calificaciones Impacto
Fuente: Autoras

NIVEL DE RIESGO	
CALIFICACION	**EXPRESIÒN**
6 o 9	Intolerable
3 o 4	Tolerable
2	Moderado
1	Aceptable

Figura 46 Calificaciones para Nivel de Riesgo
Fuente: Autoras

Ejemplo 1:

Según los esquemas de calificación que fueron planteados con anterioridad, se obtiene lo siguiente:

N° de Riesgo	RIESGO	EVALUACIÓN AL RIESGO NIVEL DE RIESGO			
		Probabilidad	Impacto	Cuantitativo	Cualitativo
43	Inexistencia de métodos para la evaluación del personal.	3	2	6	NT
45	Ausencia de planes de desarrollo-mejora de habilidades y competencias del personal de TI lo que provoca brechas en las habilidades que poseen estos respecto a las nuevas tecnologías o métodos. (INTERNO)	2	3	6	NT
51	No se encuentran claramente definidas las habilidades y competencias necesarias para ocupar un puesto en TI.	3	1	3	T

Figura 47 Evaluación del Riesgo EJ1
Fuente Autoras

El escenario de riesgo Nº 43 y 45 se califica con una probabilidad *alta* y *media* respectivamente debido a la ausencia de métodos de evaluación al personal y por ende su puesta en marcha, lo cual facilita la materialización del riesgo además evita el cumplimiento de la normativa de CI en su norma Nº410-15 así como el logro de objetivos estratégicos específicamente al OE Nº1 *Fortalecer la*

estructura organizacional aunque el primer riesgo solamente afecta al OE. Sin embargo, por la calificación que han tenido en la siguiente etapa serán objeto de priorización y tratamiento.

En relación al escenario restante, se considera su efecto únicamente en el cumplimiento del OE Nº1 más no hay relación con la normativa de CI misma que no menciona la actualización de los perfiles de un trabajador de TI conforme a los avances y necesidades del área así como la entidad en general pero su probabilidad si es *alta* debido a que el riesgo tiene facilidad de materialización.

Ejemplo 2:

Respecto a la calificación de los riesgos identificados a raíz de la carencia de un Plan de Continuidad del Negocio, se calificó de la siguiente manera:

N° de Riesgo	RIESGO	EVALUACIÓN AL RIESGO			
				NIVEL DE RIESGO	
		Probabilidad	Impacto	Cuantitativo	Cualitativo
27	Degradación de la imagen de la entidad por su incapacidad para responder oportuna y asertivamente contra incidentes que afectan a los servicios entregados por proyectos ineficientes.	1	2	2	M
68	Falta de un plan de continuidad que imposibilita responder a incidentes e interrupciones de servicios.	3	2	6	NT
146	Exposición alta a daños por ejecución de malware.	3	1	3	M

Figura 48 Evaluación del Riesgo EJ2
Fuente: Autoras

Para los tres riesgos identificados correspondientes a los N° 27, 68 y 146 se han definido los niveles de riesgo de la siguiente manera:

Para el riesgo N°27 se ha considerado que la probabilidad de ocurrencia es *bajo* debido a que la entidad cuenta con una imagen sólida como institución educativa de cuarto nivel con altos estándares de calidad en sus estudiantes, por ello el que se llegue a materializar el riesgo es poco probable; por el lado del impacto se considera una calificación de *medio* ya que la degradación de la

imagen afecta al cumplimiento del OE N° 3 esto da como resultado un nivel de riesgo *moderado.*

En relación al riesgo N°68, se ha determinado que la probabilidad de que éste se materialice es *alta* ya que la entidad carece de herramientas para encaminar su accionar al responder a incidentes que comprometan sus actividades cotidianas relacionadas con TI.

El impacto se considera *medio* ya que el plan de continuidad solo es mencionado en la norma de CI N°410-11 más no se contempla como uno de los instrumentos que permitan la consecución de los objetivos institucionales esto da como resultado un nivel de riesgo *no tolerable* para la realización de las actividades. Este riesgo por la calificación que ha tenido en la siguiente etapa será objeto de priorización y tratamiento.

Finalmente, para el riesgo N° 146 se ha determinado una probabilidad de ocurrencia *media*, debido a que existe exposición a las amenazas por parte de la institución al no contemplar la necesidad de un plan de continuidad, pero no presentan datos respecto de que las interrupciones son frecuentes y no manejadas; en relación al impacto este es *medio* ya que el riesgo solo se relaciona con el OE N°3 y no con el cumplimiento de la normativa. La calificación de nivel de riesgo es *moderado.*

Con el objetivo de presentar el panorama general de los riesgos y sus respectivos niveles, se plantea el uso de una *matriz de riesgos,* que se vuelve una herramienta fácil de manejar y entender por parte de quien analice los resultados de la gestión de riesgos.

Ejemplo 1:

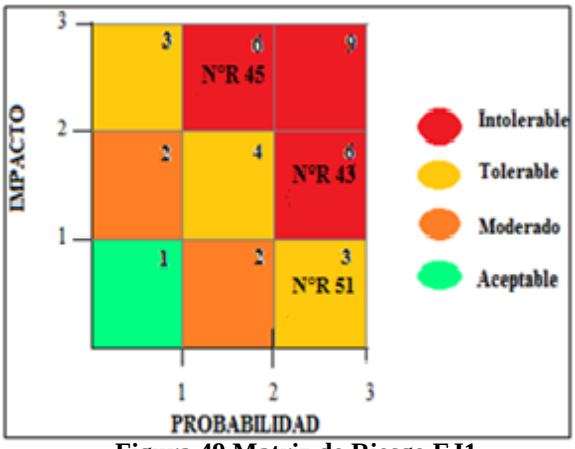


Figura 49 Matriz de Riesgo EJ1
Fuente: Autoras

Respecto de los tres riesgos de la categoría de *experiencia y habilidades del personal* se consideran que los valores asignados a la probabilidad e impacto constituyen un tipo de coordenada para ubicar el nivel de riesgo en general que la entidad presenta.

En el gráfico se puede observar que los riesgos N° 43 y 45 se ubican dentro de un nivel de riesgo alto, lo cual indica que el riesgo es *intolerable* y requiere de atención prioritaria que permita *mitigar* el mismo ya que representan obstáculos para el cumplimiento de metas y normativa respectiva.

Ejemplo 2:

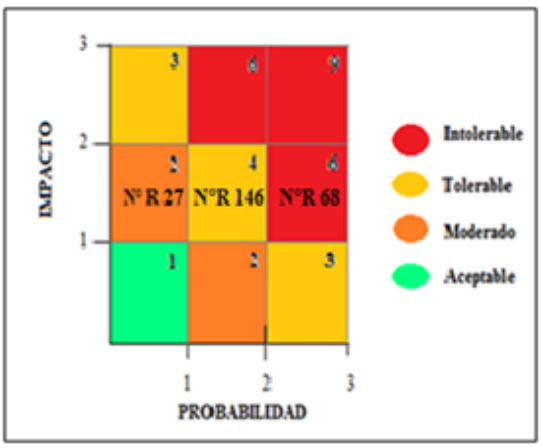


Figura 50 Matriz de Riesgo EJ2
Fuente: Autoras

Dentro del bloque *Definir la política de continuidad del negocio, objetivos y alcance* se obtuvieron tres riesgos los cuales se grafican según su probabilidad e impacto; como se puede observar en el gráfico el riesgo N° 68 con relación a los restantes se encuentra en un nivel no tolerable lo cual representa que de aquí en adelante las medidas correctivas se centrarán de manera prioritaria en el mismo.

Con el procedimiento bosquejado en los párrafos anteriores, se procede a trabajar con la totalidad de los resultados de la encuesta para obtener un portafolio de riesgos expresados en términos de probabilidad e impacto que sirva de base para proponer medidas de tratamiento conforme merezca atención el riesgo. Ver ANEXO 10.

4.3. Mantener un Perfil de Riesgo

Este paso se encuentra basado en el proceso EDM 03 cuyo aporte para nuestro análisis no es relevante, por razones mencionadas en el paso 2, las salidas que se pretende obtener mediante su aplicación, corresponden a un listado de riesgos por líneas de negocio caso no aplicado al análisis efectuado debido a que el proceso de gestión desarrollado se encuentra encaminado de manera directa a la DTIC y no a la Universidad en su conjunto.

Por otra parte, dentro de este paso se determina o se da a conocer el nivel de tolerancia y apetito al riesgo que posee la Universidad, por tal motivo para este análisis se ha tomado el mismo nivel aceptable de riesgo definido de acuerdo a los riesgos evaluados en el Plan de Mitigación de Riesgos Académicos y Administrativos de la Universidad de Cuenca.

Apetito al Riesgo: Se ha planteado que el nivel de aceptación en relación a la consecución de un objetivo es NR=P*I → NR=1*1→ NR=1 el riesgo será tolerable por lo cual no se considerarán medidas para su mitigación.

Tolerancia del Riesgo: Se considera como nivel óptimo de apetito de riesgo para las actividades, proyectos y demás de la DTIC una categoría de TOLERABLE (3-4), ya que a este nivel el riesgo es controlable con las distintas

medidas propuestas y la entidad puede soportar los riesgos en caso de que se lleguen a materializar, aclarando que las actividades deben ser adecuadamente analizadas respecto a si los beneficios a recibir superan los riesgos aceptados.

Ejemplo 1:

Con respecto a riesgos relacionados con *las experiencias y competencias del personal* calificados, todos merecen ser tratados con medidas de mitigación pues superan en nivel de tolerancia al riesgo, pero cabe mencionar que dos de estos (Nº45 y 43) no solo no están dentro del nivel de tolerancia que se ha planteado sino que sobrepasan el nivel aceptable en el desarrollo de actividades, además tienen implicaciones regulatorias lo cual es de gran importancia para la entidad, por ello el tratamiento que se dé a los riesgos debe ser prioritario y oportuno.

Ejemplo 2:

Los riesgos N° 27,68 y 146 no se encuentran, en ninguno de los casos, dentro del nivel de riesgo considerado como *aceptable*, pero se identifica que el riesgo N°68 debe ser atendido prioritariamente por considerarse como no tolerable en la realización de las actividades por parte de la entidad pues la misma no está dispuesta a asumir las consecuencias de su materialización ni tampoco tiene la capacidad para hacerlo. Los restantes riesgos se ubican dentro de los niveles *tolerable* y *moderado*, de riesgo para determinadas acciones.

4.4. Expresar el Riesgo

Los riesgos identificados deben ser dados a conocer a las partes interesadas previo a identificar y valorar las respuestas para su tratamiento, es por ello que la entidad debe adoptar o diseñar un Plan de Comunicación del Riesgo, el cual dependerá de la realidad y necesidades de cada entidad. Ver ANEXO 11.

Una vez analizados los riesgos se obtiene una plantilla en la cual se distingue por cada uno: el actor, tipo de amenaza, evento, valoración, detección y tipo de riesgo; esto servirá para presentar o dar a conocer a las partes interesadas internas o externas, y en especial a la alta dirección como el director de la DTIC

y rectorado, el estado de los riesgos en el área encargada de TI. La plantilla obtenida conjuntamente con la matriz de riesgo formará parte del Informe de Riesgos. Ver ANEXO 12.

Ejemplo 1:

Nº de Riesgo	CATEGORÍAS																					ACTOR		TIPO DE AMENAZA			EVENTO									VALORACIÓN		DETECCIÓN			TIPO DE RIESGO		
	Establecimiento y mantenimiento del portafolio	Gestión del ciclo de vida del programa o proyecto	Decisión de hacer Inversión TI	Experiencia y habilidades en TI	Información (Violación de datos: daños, fuga y acceso)	Arquitectura	Infraestructura	Software	Propiedad de un negocio de TI	Proveedores	Cumplimiento regulatorio	Robo o destrucción de infraestructura	Malware	Ataques lógicos	Acción industrial	Ambiente	Hechos de la naturaleza	Innovación	Interno	Externo	Malicioso	Error	Falla	Revelación	Interrupción	Modificación	Robo	Destrucción	Diseño Inefectivo	Leyes y Regulación	Uso Inapropiado	Recurso	Activo	Lenta	Moderada	Instantánea	Beneficio de TI/ Habilitación de	Programa de TI y proyecto	Operaciones de Servicios de TI
43				■															■				■						■			■				■	S		P
45				■															■				■							■		■		■			S	S	P
51				■															■			■						■			■		■			S	S	P

Figura 51 Informe del Riesgo EJ1
Fuente: Autoras

Para ilustración en el escenario N° 43 pertinente a la categoría del escenarios *experiencia y habilidades de TI*, el riesgo afecta directamente al personal de la entidad por lo que el actor es *interno* y su origen se centra en un *falla* ya que no se ha contemplado la necesidad de métodos de evaluación al personal de TI dentro de la definición de políticas y procedimientos. El evento se relaciona con un *diseño inefectivo.*

El personal constituye un *recurso* para la entidad pues mediante las acciones que realicen son un medio para la materialización de las metas institucionales previamente fijadas y dadas o conocer pero así como su efecto es positivo con una adecuada gestión puede actuar en contra de ello. La materialización del riesgo es *instantánea* ya que simplemente existe o no un método de evaluación al personal, esto con la identificación o revisión física.

Finalmente, se considera que el riesgo afecta a *las operaciones de servicios de TI* ya que si el personal no está preparado y no es periódicamente evaluado, no se podrán detectar aquellas falencias respecto al manejo de nuevas

soluciones implementadas lo que llevaría a no aprovecharlas afectando directamente a la construcción de valor para la entidad e incluso aportaría a la destrucción del actualmente existente. También se puede mencionar que el personal puede causar daños que repercutan en la entrega de los servicios esto relacionado con el manejo o configuración de software.

Respecto al riesgo N°45 y sus atributos, difiere con respecto al anterior, con respecto del evento ya que éste se relaciona con *leyes y normativa* así como también en la detección que sería *lenta* pues se tendrían que desencadenar desviaciones graves que se relacionen con el personal para analizar la estructura definida incluyendo políticas y procedimientos en donde se detecte la carencia de un plan de formación.

El último de los riesgos identificados para el bloque difiere en el atributo *tipo de amenaza* ya que el riesgo se generaría por un *error* que implique formulación de políticas confusas o sistemas de comunicación erróneos.

Ejemplo 2:

Nº de Riesgo	CATEGORÍAS																					ACTOR		TIPO DE AMENAZA			EVENTO									VALORACIÓN		DETECCIÓN			TIPO DE RIESGO		
	Establecimiento y mantenimiento del portafolio	Gestión del ciclo de vida del programa o proyecto	Decisión de hacer Inversión TI	Experiencia y habilidades en TI	Información (Violación de datos: daños, fuga y acceso)	Arquitectura	Infraestructura	Software	Propiedad de un negocio de TI	Proveedores	Cumplimiento regulatorio	Robo o destrucción de infraestructura	Malware	Ataques lógicos	Acción industrial	Ambiente	Hechos de la naturaleza	Innovación	Interno	Externo	Malicioso	Error	Falla	Revelación	Interrupción	Modificación	Robo	Destrucción	Diseño Inefectivo	Leyes y Regulación	Uso Inapropiado	Recurso	Activo	Lenta	Moderada	Instantánea	Beneficio de TI/ Habilitación de	Programa de TI y proyecto	Operaciones de Servicios de TI
27		■																																		P	S	S
68					■														■	■	■			■								■			■		S	S	P
146													■							■	■						■					■		■			P	S	S

Figura 52 Informe del Riesgo EJ2
Fuente: Autoras

El riesgo N° 27 se ubica en la categoría *Gestión del ciclo de vida del programa o proyecto,* los actores dependerán de las actividades que se realicen existiendo tanto personal *interno* (administrativos, docentes, etc.) como el *externo* (estudiantes, proveedores, etc.) así como las demás partes relacionadas.

Este riesgo surge por la *falla* en la gestión de los proyectos lo cual se detecta mediante *revelaciones* que se generan por las opiniones u observaciones de personas lo que puede desfavorecer la imagen de la entidad, esto no es fácilmente detectable por lo que se considera un nivel *lento* para su identificación llegando a ser finalmente un *recurso* útil para la obtención de valor en sus servicios ofertados.

Para el riesgo N° 68 que corresponde a la *Información,* por lo que la ausencia del Plan de Continuidad se puede generar diversos daños en la integridad, oportunidad y relevancia de la misma. Dichos riesgos pueden provenir de una fuente tanto *interna* como *externa* llegando a representar una amenaza *maliciosa* considerando que es la materia prima para el proceso administrativo*;* el evento relacionado a su descubrimiento es la *revelación* proporcionada por la DTIC de que algo ha ocurrido con la información y no están preparados para responder a ello, llegando así a la conclusión de que el diseño y uso de dicho plan representa un *recurso* para el debido cuidado tanto de la información como de los activos físicos relacionados.

Para concluir con el análisis de la plantilla, el riesgo N° 146 se lo identifica dentro de la categoría de *malware* por la falta de políticas que especifique los procedimientos para el tratamiento de los riesgos ocasionados por cambios en los proyectos, los actores se consideran del entorno *externo* representados por los avances y mejoras tecnológicas lo que provoca que su desactualización facilite al *robo* de información o datos considerados como sensibles, al ser de este modo su detección correspondiente no es inmediata, es decir, es *lenta* ya que dependerá de la ocurrencia de algún suceso importante para que se proceda a realizar los análisis necesarios.

4.5. Definición de un Portafolio de Acciones para la GR

Se procede a la identificación de las acciones necesarias para reducir el riesgo entre el nivel aceptable y la tolerancia al riesgo, para ello se determinan actividades de COBIT 5 *Procesos Catalizadores* que permitan tratar los riesgos

y ayudar a la entidad a cumplir los objetivos estratégicos considerados para el área que maneja las TIC.

A la vez, se busca satisfacer el marco regulatorio; esto únicamente enfocado a los riesgos prioritarios (calificados como NT).

Para cada uno de los riesgos se ha considerado la necesidad de describir las *actividades* que se deben llevar a cabo para poder tratar el riesgo, los *responsables* desde dos puntos de vista: la persona que es responsable de poner en práctica las acciones y quién es la encargada de rendir cuentas por la realización de las mismas; así también por cada uno de estos se diferencia a responsables que están específicamente relacionados con el área de la DTIC y otros que pertenecen a la Universidad en su conjunto.

Se detallan además los recursos necesarios para la implementación y las métricas necesarias para definir la efectividad de las actividades; finalmente se llega a establecer el nivel de riesgo residual fruto de la aplicación de las acciones. Ver ANEXO 13.

Ejemplo 1-2:

N°	RIESGO	NIVEL DE RIESGO		ACTIVIDADES							
				DESCRIPCIÓN	RECURSOS				RESPONSABLES		MÉTRICAS RELACIONADAS
		CUANTITATIVO	CUALITATIVO		Información	Aplicaciones	Infraestructura	Personas	RESPONSABLE* ¿Quién hace?	RINDE CUENTAS* ¿Quién comunica?	
45	Ausencia de planes de desarrollo-mejora de habilidades y competencias del personal de TI lo que provoca brechas en las habilidades que poseen estos respecto a las nuevas tecnologías o métodos. (INTERNO)	6	NT	Identificar las competencias y habilidades requeridas así como existentes, que apoyan la consecución de objetivos para luego plantear los planes de desarrollo y formación del personal basados en dichos resultados; de esta manera estos serán objetivos.	X			X	INSTITUCIÓN: Coordinador/a Administrativo de la Unidad de Planificación física y ejecución de obras, Director de Talento Humano DTIC: Coordinador de Sistemas de Información, Ingeniero 3 Unidad de Centro de Desarrollo de Software, Ingeniero 3 Unidad de Operaciones de Sistemas Informáticos, Ingeniero 2 Infraestructura de TI, Ingeniero 3 de Servicios de CSE, Ingeniero 3 de Seguridad CRC	Director de TIC	Número de empleados de la D TIC evaluados/Total de empleados de la DTIC. Número de propuestas ejecutadas/Número de propuestas ejecutadas. Número de horas de formación reales/Número de horas planeadas de formación
43	Inexistencia de métodos para la evaluación del personal.	6	NT	Aplicación de una evaluación de desempeño 360° y desarrollar planes de mejora basados en los resultados de la evaluación así como de las brechas identificadas del personal.				X	INSTITUCIÓN: Director de Planificación, Director de Talento Humano DTIC: Ingeniero 3 Unidad de Centro de Desarrollo de Software, Ingeniero 3 Unidad de Operaciones de Sistemas Informáticos, Ingeniero 3 de Servicios, Ingeniero 3 de Seguridad.	Coordinador de Sistemas de Información	Porcentaje de puestos vacantes. Frecuencia de las evaluaciones del personal entrante como antiguo.
68	Falta de un plan de continuidad que imposibilita responder a incidentes e interrupciones de servicios.	6	NT	Desarrollar políticas de continuidad de negocio. Diseñar e implementar un Plan de Continuidad de Negocio que partirá de un análisis de riesgo de los procesos críticos del negocio lo cual permitirá definir las estrategias que se adoptarán para evitar la interrupción de operaciones definiendo, responsables, recursos, acciones, pruebas, mantenimiento y revisión de dicho plan. Además incluir en el plan de comunicación los aspectos específicos para casos emergentes.	X	X	X	X	INSTITUCIÓN: Coordinador/a de la Unidad de Planificación Estratégica, Unidad de Auditoría Interna DTIC: Director de TIC, Coordinador de Sistemas de Información, Ingeniero 2 Infraestructura de TI	Coordinador/a de la Unidad de Control	Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos. Número de interrupciones del negocio debidas a incidentes en el servicio de TI. Porcentaje de mejoras acordadas que han sido reflejadas en el plan. Porcentaje de asuntos identificados que se han incluido satisfactoriamente en el plan.

Figura 53 Acciones para tratar el Riesgo

*Adaptado al orgánico funcional de la Universidad de Cuenca y de la DTIC.
Fuente: Autoras

Para los bloques tratados con el fin de ejemplificar el proceso de Gestión de Riesgos se ha obtenido esta plantilla final, en la cual se encuentran definidos ítems relevantes y concisos en la implementación de acciones a tomar para tratar riesgos, siendo de utilidad para el encargado e informativo para otras partes.

En los riesgos pertenecientes al bloque de *experiencias y habilidades* la rendición de cuentas respecto de las actividades estará a cargo del director de DTIC en el caso de la formulación de planes enfocados a la formación y desarrollo del personal con el propósito de mantener la actualización y mejora continua de sus habilidades y competencias; y por otra parte está el Coordinar de Sistemas de información para las evaluaciones del desempeño.

Igualmente se han definido los recursos necesarios para ejecutar las acciones en los que se contemplan *información* y *personas* en el caso de los planes, esto debido a que para establecer los mismos adecuadamente se necesita de información objetiva y concisa de la situación real y las necesidades de la DTIC en relación al personal. Adicionalmente el personal será quien interactúe con los encargados de la definición de planes para presentar sus puntos de vista y será a quienes se evalúe posteriormente.

Las métricas se enfocan a las actividades planteadas, al ser una herramienta para medir el porcentaje en el que las mismas se han desarrollado y han cumplido con los objetivos.

Para el riesgo identificado en el bloque de *Plan de Continuidad,* las actividades para contrarrestarlo dependerán inicialmente del diseño inmediato de políticas enmarcadas hacia a la continuidad de sus operaciones para posteriormente planear, diseñar e implementar propiamente un Plan de Continuidad de Negocio considerando la necesidad de contemplar los siguientes recursos: *información, aplicaciones, infraestructura y personas,*

Esto se basará primeramente en la identificación y análisis de los procesos claves de TI para la entidad, con el objetivo que se facilite conocer en qué se debe enfocar la atención y posteriormente establecer los criterios a seguir, para

que de este modo en cualquier adversidad no se congelen las actividades de la entidad, sino que inmediatamente se proceda a implantar lo que se detalle en el plan. La persona quién rendirá cuentas de las actividades realizadas para el tema es el Coordinador/a de la Unidad de Control, mismo que empleará para mayor facilidad y visualización de los logros conseguidos las métricas señalas.

Finalmente, se considera la evaluación o definición del nuevo nivel de riesgo de la entidad en relación con los riesgos priorizados. Ver ANEXO 16.

N°	RIESGO	NIVEL DE RIESGO		RIESGO RESIDUAL CÁLCULO		
		CUANTITATIVO	CUALITATIVO	Impacto	Probabilidad	Riesgo Residual
45	Ausencia de planes de desarrollo-mejora de habilidades y competencias del personal de TI lo que provoca brechas en las habilidades que poseen estos respecto a las nuevas tecnologías o métodos. (INTERNO)	6	NT	1	2	2
43	Inexistencia de métodos para la evaluación del personal.	6	NT	1	2	2
68	Falta de un plan de continuidad que imposibilita responder a incidentes e interrupciones de servicios.	6	NT	1	3	3

Figura 54 Riesgo Residual
Fuente: Autoras

Como se puede apreciar, los niveles de riesgo se han reducido para los tres riesgos a: *moderado(N°43-45)* y *aceptable* (N°68); ello como resultado de las actividades propuestas y la confianza determinada para éstas. Cabe destacar que la probabilidad se ha re-evaluado nuevamente en base a las medidas planteadas lo cual no ocurre con el impacto, pues el riesgo como tal sigue afectando, con la posible materialización, a los objetivos institucionales, la normativa de Control interno o ambos.

Con la obtención del nivel de riesgo residual se puede realizar una comparación con el nivel de riesgo actual, de manera que se observen los efectos posteriores al decidir implementar las acciones para el tratamiento del

riesgo así como plantear una nueva matriz de riesgo. Ver ANEXO 17 y 18.

4.6. Respuesta al Riesgo

Finalmente, el análisis anteriormente realizado sobre la gestión de riesgos concluye en la presentación del Plan de Acciones para el Tratamiento de los Riesgos, en el que se sintetiza los riesgos con su respectivo nivel, las actividades, responsables e indicadores para evaluar la eficiencia de dichas medidas. Adicionalmente se define el nivel de respuesta al riesgo que se va a alcanzar con las acciones propuestas en el caso de ser implementadas. Ver ANEXO 19.

Ejemplo 1-2:

N° de Riesgo	RIESGO	RESPUESTA			
		Aceptar	Transferi	Mitigar	Evitar
45	Ausencia de planes de desarrollo-mejora de habilidades y competencias del personal de TI lo que provoca brechas en las habilidades que poseen estos respecto a las nuevas tecnologías o métodos. (INTERNO)			X	
43	Inexistencia de métodos para la evaluación del personal.		X		
68	Falta de un plan de continuidad que imposibilita responder a incidentes e interrupciones de servicios.		X		

Figura 55 Respuesta al Riesgo
Fuente: Autoras

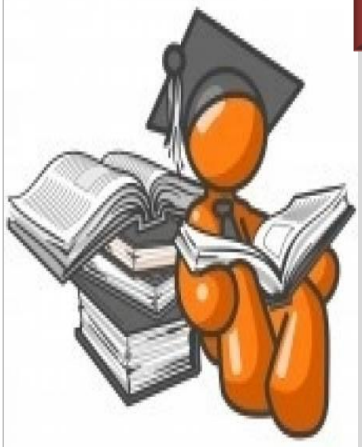
En el caso del riesgo N° 45 se pretende disminuirlo, es decir, MITIGARLO con el empleo y ejecución de las actividades propuestas mientras que para el riesgo N° 43 la propuesta se enfoca en el uso de una evaluación de 360° para lo cual se deberá optar por TRANSFERIR dicha actividad a profesionales expertos en el tema para direccionar el tiempo de estas a aquellas denominadas actividades distintivas que le permiten a la entidad incrementar su capacidad y competitividad a nivel del servicio que ofrece.

En el caso del riesgo N°68 las actividades planteadas tienden a disminuirlo y la repuesta con la aplicación de dichas acciones será la MITIGACIÓN.

Con este paso culmina el proceso de Gestión de Riesgos, obteniendo como productos finales:

1. Definición de la Metodología de Gestión de Riesgos
2. Plantilla para Plan de Comunicación
3. Plantillas de Evaluación del Riesgo
4. Informe de Riesgos
5. Plan de Acciones para Tratamiento de los Riesgo de la DTIC

CAPÍTULO V



CONCLUSIONES Y RECOMENDACIONES

Daisy Fernanda Alvarado Carpio
Laura Alexandra Zumba Morales

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Mediante el análisis desarrollado se puede cotejar que la adopción de estándares o marcos internacionales enfocados en la Gestión de Riesgos de las TIC son poco conocidos o si bien es cierto han pasado desapercibidos para las entidades en nuestro medio, que al pasar de los años han venido acogiéndose a procedimientos rutinarios que imposibilitan su desarrollo o desempeño eficaz así como generar beneficios de manera global.

La Universidad de Cuenca como ente educativo reconocido requiere que sus niveles de administración de las tecnologías sean óptimos de manera que le permitan solventar eventualidades oportunamente y lograr bienestar no solo de sus partes interesadas externas sino de todas aquellas que intervienen en la realización de actividades diarias.

Por lo mencionado, se considera a la Gestión de Riesgos como una herramienta que asegura la continuidad del negocio y que puede ser implementada en cualquier tipo de entidad independientemente de su naturaleza. El marco de referencia *COBIT 5* y sus productos: *COBIT 5 para Riesgos* y *COBIT 5 Procesos Catalizadores* permiten mediante su implementación, ya sea desde la perspectiva de función del riesgo o gestión del riesgo; lograr una identificación y tratamiento de los riesgos enfocados en el uso de la tecnología para la entrega de servicios y realización de actividades o procesos en general teniendo como bases los objetivos institucionales así como las normas legales vigentes.

El Proceso de Gestión de Riesgos planteado por *COBIT 5 para Riesgos* compuesto por seis etapas guarda estrecha relación con estándares como ISO 31000 – 27005; pero destacándose por consideraciones específicas en las etapas de: *análisis de riesgo* por el trabajo con escenarios de riesgos así como *expresar el riesgo* al contemplar un plan de comunicación de riesgos y el manejo de informes al respecto.

A través de la evaluación de riesgos aplicada conforme la metodología propuesta por *COBIT 5 para Riesgos,* se ha podido determinar que la DTIC presenta aspectos débiles en la gestión de riesgos con respecto a la normativa de Control Interno.

Dentro de estos aspectos se destacan: la ausencia de un Código de Conducta que permita a todos los servidores del área desempeñarse dentro de pautas y delimitaciones previamente establecidas, otro tema que desencadena una serie de vulnerabilidades es la ausencia de un adecuado ciclo de vida de sus proyectos destacándose una carencia de comunicación continua con las altas unidades académicas así como con los usuarios, para determinar si las inversiones han sido las idóneas, en otras palabras podemos detallar que se detectó el desconocimiento de aspectos claves en cuanto a planes de riesgos e informes de satisfacción de usuarios dando como resultado la ausencia de seguimiento de lo ejecutado, lo cual está relacionado con la falta de control de calidad en sus servicios. También se destaca la ausencia de un Plan de Continuidad del Negocio que permita la adopción oportuna de acciones ante imprevistos que causen interrupción en la prestación de servicios de la entidad.

Los riesgos de la DTIC se encuentran gestionados mediante la consideración de prácticas presentadas por *COBIT 5 Procesos catalizadores*, en donde se establece las actividades que se debe efectuar con el fin de disminuir las deficiencias de la DTIC en cuanto a temas relacionados con el cumplimiento normativo y aquellos que imposibilitan el logro de sus objetivos, de esta manera cada práctica analizada permite disponer de información que representa salidas o entradas dependiendo de los aspectos analizados cómo se pudo apreciar en el análisis efectuado a lo largo de este trabajo.

Cabe recalcar que al concluir el análisis conforme la metodología propuesta, se obtienen diferentes productos que instrumentalizan su accionar entre estos quizá el más importante por su objetivo de tratar los riesgos es el Plan de Mitigación de Riesgos, en el cual se proponen diversas actividades y responsables para manejar aquellos aspectos así como el detalle de métricas

que permitan comprobar la eficiencia y eficacia en el control de los niveles de riesgos de las TIC.

Los beneficios resultantes de la aplicación de este proceso para la DTIC no solo se encuentran direccionados al cumplimiento de leyes, reglamentos, regulaciones y políticas cuyo fin fue la realización de la presente tesis; sino que adicionalmente permite lograr una alineación estratégica, debido a su aporte para la creación de valor al relacionarse directamente con la Alta Dirección lo cual se vincula con el fortalecimiento de la comunicación para la toma de decisiones en pro de la Universidad en sí, con un enfoque hacia la maximización de la satisfacción en los usuarios.

5.2. Recomendaciones

COBIT 5 es aplicado en universidades, y empresas en general, de gran prestigio a nivel mundial por su adaptabilidad y beneficios, lo que les ha permitido sostener y mejorar sus actividades y servicios, pues se convierte en una marco de referencia que combina diferentes aspectos relacionados a gestión de: riesgos, calidad, talento humano entre otros vinculando aspectos internos y externos como regulaciones vigentes que afecten directa o indirectamente a TI y su entorno.

De lo analizado, aplicado y concluido en páginas anteriores, se considera apropiada y necesaria la adopción de *COBIT 5 para Riesgos* dentro de la DTIC de la Universidad de Cuenca como metodología para tratar estos; pero además se considera importante que la entidad implemente: las estructuras y los procesos para el Gobierno Empresarial de TI contemplados por *COBIT 5* mediante la instrumentalización e implementación de las actividades detalladas en las prácticas direccionadas a los siete catalizadores.

La implementación total de la estructura, asegura la cobertura de todos los elementos necesarios para un óptimo funcionamiento de la entidad y consecución de objetivos; logrando equilibrio y coherencia entre: principios, políticas y marco de trabajo, procesos de la entidad, estructura organizacional,

cultura, ética y comportamiento de las personas; información, servicios, infraestructura y aplicaciones, y finalmente como elemento principal las personas conjuntamente con sus habilidades y competencias.

De esta manera el proceso de *gestión y gobierno de TI* se volverá participativo y permitirá estructurar, detectar así como priorizar el tratamiento de los riesgos que impiden alcanzar los beneficios relacionados con el uso de TI tales como: optimizar recursos, manejar proyectos, asegurar las características de la información y la generación de valor agregado, principalmente. La entidad podrá mejorar su desempeño institucional adaptándose al entorno cambiante en el cual se desenvuelve y a la vez cumplirá con su objetivo de convertirse en una *universidad de docencia con investigación* ubicándose en el área de excelencia académica al nivel de universidades del llamado primer mundo.

ABREVIATURAS

CMI: Cuadro de Mando Integral

CI: Control Interno

DMAIC: Definir, Medir, Analizar, Mejorar, Controlar

DTIC: Dirección de Tecnologías de Información y Comunicación

EJ: Ejemplo

H.C: Honorable Consejo

IES: Institutos de Educación Superior

NR: Nivel de Riesgo

OE: Objetivo Estratégico

PEUC: Plan Estratégico Institucional de la Universidad de Cuenca

PNBV: Plan Nacional del Buen Vivir

POA: Plan Operativo Anual

SLA: Service Level Agreement (Acuerdo de Nivel de Servicio)

TIC: Tecnologías de Información y Comunicación

UC: Universidad de Cuenca

GLOSARIO

Acuerdo de Nivel de Servicio (SLA).- EL modelo de Acuerdo de Nivel de Servicios (Service Level Agreement, SLA) consiste en un contrato en el que se estipulan los niveles de un servicio en función de una serie de parámetros objetivos, establecidos de mutuo acuerdo entre ambas partes, así, refleja contractualmente el nivel operativo de funcionamiento, penalizaciones por caída de servicio, limitación de responsabilidad por no servicio, etc.

Este modelo no ha de estar relacionado necesariamente con la contratación de servicios a terceras partes, sino que puede implantarse a nivel interno, transformando una determinada unidad de negocio en centro de servicios que provea a la propia compañía. Se describe y obliga a un nivel específico de calidad en el suministro. (Abogados Portaley, 2015)

Arquitectura de Información.- es la disciplina encargada del estudio, análisis, planificación y fundamentación de la organización, disposición y estructuración de espacios de información, y de la selección y presentación de los datos contenidos en los sistemas de información interactivos. (Varios, Alegsa, 2014)

Arquitectura de Procesos.- La arquitectura de procesos en general identifica que procesos definen una estructura funcional y se anticipa al proceso mismo. Define una guía que minimiza todo riesgo inherente durante el desarrollo de proyectos. (AwE, 24)

Buena Práctica.- Toda experiencia que se guía por principios, objetivos y procedimientos apropiados o pautas aconsejables que se adecuan a una determinada perspectiva normativa o a un parámetro consensuado, así como también toda experiencia que ha arrojado resultados positivos, demostrando su eficacia y utilidad en un contexto concreto. (Be, 2015)

Cadena De Valor.- Se conoce como cadena de valor a un concepto teórico que describe el modo en que se desarrollan las acciones y actividades de una

empresa. En base a la definición de cadena, es posible hallar en ella diferentes eslabones que intervienen en un proceso económico: se inicia con la materia prima y llega hasta la distribución del producto terminado. En cada eslabón, se añade valor, que, en términos competitivos, está entendido como la cantidad que los consumidores están dispuestos a abonar por un determinado producto o servicio. (Varios, Definición de, 2015)

Contingencia.- Posibilidad de que algo suceda o no suceda. (RAE, 2015)

Continuidad.- Cualidad o condición de las funciones o transformaciones continúas**.** (RAE, 2015)

Clúster: Un clúster está formado por dos o más servidores independientes pero interconectados. Algunos clústeres están configurados de modo tal que puedan proveer alta disponibilidad permitiendo que la carga de trabajo sea transferida a un nodo secundario si el nodo principal deja de funcionar. Otros clústeres están diseñados para proveer escalabilidad permitiendo que los usuarios o carga se distribuya entre los nodos. Ambas configuraciones son consideradas clústeres. (García, 2008)

Efectividad.- Capacidad de lograr el efecto que se desea o se espera. (RAE, 2015)

Eficiencia.- Capacidad de disponer de alguien o de algo para conseguir un efecto determinado. (RAE, 2015)

Hacker.- Término utilizado para llamar a una persona con grandes conocimientos en informática y telecomunicaciones y que los utiliza con un determinado objetivo. Este objetivo puede o no se maligno o ilegal. La acción de usar sus conocimientos se denomina hacking o hackeo. (Varios, Alegsa)

Indexar.- Registrar ordenadamente datos e informaciones, para elaborar su índice. (RAE, 2015)

Infraestructura de TI.- La infraestructura de TI de una empresa no solo hace referencia a la red, los servidores o las aplicaciones, sino también a los clientes,

los dispositivos móviles y los servicios individuales. La interacción fluida de todos estos componentes contribuye de forma significativa al éxito de su empresa. (Comparex, 2015)

Mitigación.- Moderar, aplacar, disminuir o suavizar algo riguroso o áspero. (RAE, 2015)

Programa.- Agrupan proyectos relacionados, que pueden ser ejecutados de manera secuencial o paralela. (Nakamura, 2015)

Proyecto.- Se dan cuando existen actividades nuevas, incluyendo mejoras nuevas. Tienen un inicio y fin, objetivos específicos, entregables y son únicos. (Nakamura, 2015)

Portafolio.- Una colección de programas y proyectos que pueden estar o no interrelacionados. La persona que maneja un portafolio puede ser llamada Director o Vicepresidente, dado que este tipo de trabajo involucra la dirección de todo el trabajo, gente, presupuesto, proveedores, etcétera. (Nakamura, 2015)

Reingeniería Social.- Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social. (Symantec)

Rootkits.- Componente de malware que utiliza la clandestinidad para mantener una presencia persistente e indetectable en un equipo. Las acciones realizadas por un rootkit, como la instalación y diversas formas de ejecución de códigos, se realizan sin el conocimiento o consentimiento del usuario final.

Los rootkits no infectan las máquinas por sí mismos como lo hacen los virus o gusanos, sino que tratan de proporcionar un entorno indetectable para ejecutar códigos maliciosos. Los atacantes normalmente aprovechan las vulnerabilidades en el equipo seleccionado o utilizan técnicas de ingeniería social para instalar manualmente los rootkits. O, en algunos casos, los rootkits pueden instalarse

automáticamente al ejecutarse un virus o gusano o incluso simplemente al navegar en un sitio Web malicioso.

Una vez instalados, el atacante puede realizar prácticamente cualquier función en el sistema, incluyendo acceso remoto, intercepción de comunicaciones, así como procesos de ocultamiento, archivos, claves de registro y canales de comunicación. (Symantec)

Spyware.- Paquete de software que realiza un seguimiento y envía información de identificación personal o información confidencial a otras personas. La información de identificación personal es la información que puede atribuirse a una persona específica, como un nombre completo. La información confidencial incluye datos que la mayoría de personas no estaría dispuesta a compartir con nadie e incluye datos bancarios, números de cuentas de tarjeta de crédito y contraseñas. Los receptores de esta información pueden ser sistemas o partes remotas con acceso local. (Symantec)

Virus.- Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios:

- Debe ejecutarse por sí mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa.
- Debe reproducirse: por ejemplo, puede reemplazar otros archivos ejecutables con una copia del archivo infectado por un virus. Los virus pueden infectar computadores de escritorio y servidores de red.

Muchos de los virus actuales están programados para operar sigilosamente la computadora del usuario con el fin de robar información personal y utilizarla para cometer delitos. (Symantec)

ANEXOS

Daisy Fernanda Alvarado Carpio
Laura Alexandra Zumba Morales

Anexo 1: Riesgos y Acciones del Plan de mitigación de riesgos de la Dirección de Desarrollo Informático

N°	RIESGO	ACCIONES
1	¿Cuál es la probabilidad que la DDI no cuente con una estructura orgánica funcional?	Redefinir la estructura organizacional de la DDI para mejorar la atención y cobertura de servicios informáticos de la Universidad de Cuenca.
2	¿Cuál es la probabilidad que las TIC no sean consideradas en la toma de decisiones, estratégicas y en la planificación institucional?	Definir Políticas de Tecnologías de Información y Comunicaciones (TIC) de la Universidad de Cuenca.i). Elaborar las Políticas de las TIC.ii. Elaborar un documento de Políticas de Seguridad de las TIC.
3	¿Cuál es la probabilidad que no se evalúen los servicios de TIC en la U.C.?	Elaborar las normativas necesarias para el funcionamiento seguro y con calidad de la DDI. i) Elaborar el Manual de Procedimientos de la DDI para una adecuada operación de los servicios informáticos. ii). Elaborar un Manual de Gestión de Proyectos de TIC. iii) Reglamento de responsabilidad y uso de la firma electrónica.
4	¿Cuál es la probabilidad que no se cuenten con procedimientos para especificar las funciones del personal de la DDI así como también de políticas regulatorias para los usuarios de la TIC?	
5	¿Cuál es la probabilidad que no se aplique un procedimiento de evaluación de desempeño del personal de la DDI, que nos permita supervisar funciones y cumplimiento de roles para optimización y fortalecimiento?	Evaluar las funciones y desempeño del personal informático de la DDI y de Facultades.i) Elaborar el Manual de Funciones del personal de la DDI para el funcionamiento seguro y con calidad de la Dirección.ii) Evaluar las funciones y desempeño del personal informático de la DDI y de Facultades.
6	¿Cuál es la probabilidad que la planificación estratégica aplicada en la DDI no esté definida, presupuestada, legalizada, difundida, implementada, evaluada y no esté alineada y estructurada de acuerdo al plan estratégico institucional?	Rediseñar y alinear los servicios informáticos a las políticas y necesidades de crecimiento institucional. Elaborar el Plan Estratégico de TIC alineado los servicios informáticos a las políticas y necesidades de crecimiento institucional
7	¿Cuál es la probabilidad que plan operativo anual de la DDI no esté definido, presupuestado, legalizado, difundido, implementado, evaluado y no este alineado y con los requerimientos del estratégico institucional?	Rediseñar y alinear los servicios informáticos a las políticas y necesidades de crecimiento institucional.Rediseñar y alinear el Plan Operativo Anual de los servicios informáticos a las políticas y necesidades de crecimiento institucional.
8	¿Cuál es la probabilidad de no contar con políticas, procedimientos debidamente estructurados, pertinentes, implementados y difundidos para la gestión de las TIC, que incluyan temas como: Asignación y aprobación de personal e infraestructura, regulación de actividades, políticas de administración de procesos, sistemas de aseguramiento de calidad, de gestión de riesgo y estándares tecnológicos?	Implementar procedimientos y actividades para una adecuada operación de los servicios informáticos.i) Dispone de un Procedimiento de respaldos de información de servidores centrales en donde se especifique cronograma, custodios, lugares de almacenamiento externo.ii) Implementar un Sistema de Gestión de Incidentes de seguridad (CSIRT) de las TIC.iii) Implementar el Plan de Gestión de Riesgos de la DDI.
9	¿Cuál es la probabilidad que los convenios y contratos de servicios e infraestructura informáticos, adquiridos no están debidamente controlados?	Implementar procedimientos y actividades para una adecuada operación de los servicios informáticos.i) Dispone de un Procedimiento de respaldos de información de servidores centrales en donde se especifique cronograma, custodios, lugares de almacenamiento externo.ii) Implementar un Sistema de Gestión de Incidentes de seguridad (CSIRT) de las TIC.iii) Implementar el Plan de Gestión de Riesgos de la DDI.Generar un Plan de Adquisición de Infraestructura Tecnológica de acuerdo con la planificación operativa y las necesidades institucionales.
10	¿Cuál es la probabilidad de no contar con un modelo de datos en el que se considere la definición del modelo, los procesos y procedimientos de manejo de información; que incluya reglas de validación, control, integridad, identificando los diferentes niveles de seguridad y propiedad; además, que no cuente con un diccionario de datos corporativo actualizado y documentado?	Elaborar las normativas necesarias para el funcionamiento seguro y con calidad de la DDI.i) Elaborar el Manual de Procedimientos de la DDI para una adecuada operación de los servicios informáticos.ii). Elaborar un Manual de Gestión de Proyectos de TIC.iii) Reglamento de responsabilidad y uso de la firma electrónica.

11	¿Cuál es la probabilidad de no calcular el costo total propiedad o que no se incluyan todos los costos?	Implementar proceso de mejora continua en la prestación de los servicios informáticos. i) Se dispone de un Sistema de control de acceso y seguridad física de la DDI. ii) Elaborar un Procedimiento de creación y baja de usuarios de los sistemas y servicios informáticos.iii) Disponer de un repositorio de documentos técnicos de la DDI que faciliten la gestión y operación de las TIC. Elaborar un Manual de Gestión de Proyectos de TIC.
12	¿Cuál es la probabilidad de no contar con administrador de proyectos de TIC?	Implementar proceso de mejora continua en la prestación de los servicios informáticos. i) Se dispone de un Sistema de control de acceso y seguridad física de la DDI.ii) Elaborar un Procedimiento de creación y baja de usuarios de los sistemas y servicios informáticos.iii) Disponer de un repositorio de documentos técnicos de la DDI que faciliten la gestión y operación de las TIC. Elaborar un Manual de Gestión de Proyectos de TIC.
13	¿Cuál es la probabilidad de no contar con lineamientos, procedimientos, y metodología para el desarrollo, mantenimiento y/o adquisición de software aplicativo, que contengan parámetros de calidad, fiabilidad y disponibilidad?	Fortalecer el Centro de Desarrollo de Software.i) Revisar y mejorar los lineamientos, procedimientos, y metodología para el desarrollo, mantenimiento y/o adquisición de software. ii) Elaborar el Modelo de Datos de la Universidad de Cuenca que incluya las reglas de validación, control, integridad, y diccionario de datos.ii) Elaborar el Modelo de Datos de la Universidad de Cuenca que incluya las reglas de validación, control, integridad, y diccionario de datos.
14	¿Cuál es la probabilidad de que en los contratos de adquisición de software no se consideren los aspectos técnicos de los productos, licencias de uso y servicio, garantías contractuales, soporte y mantenimiento?	Implementar procedimientos y actividades para una adecuada operación de los servicios informáticos. i) Dispone de un Procedimiento de respaldos de información de servidores centrales en donde se especifique cronograma, custodios, lugares de almacenamiento externo. ii) Implementar un Sistema de Gestión de Incidentes de seguridad (CSIRT) de las TIC. iii) Implementar el Plan de Gestión de Riesgos de la DDI.
15	¿Cuál es la probabilidad de que en la implementación del software no se cumplan los aspectos contractuales de configuración, validación, aceptación y documentación?	Implementar procedimientos y actividades para una adecuada operación de los servicios informáticos. i) Dispone r de un Procedimiento de respaldos de información de servidores centrales en donde se especifique cronograma, custodios, lugares de almacenamiento externo. ii) Implementar un Sistema de Gestión de Incidentes de seguridad (CSIRT) de las TIC. iii) Implementar el Plan de Gestión de Riesgos de la DDI.
16	¿Cuál es la probabilidad de que no se registre los derechos de autor cuando se desarrolle software aplicativo a la medida?	Fortalecer el Centro de Desarrollo de Software.i) Revisar y mejorar los lineamientos, procedimientos, y metodología para el desarrollo, mantenimiento y/o adquisición de software. ii) Elaborar el Modelo de Datos de la Universidad de Cuenca que incluya las reglas de validación, control, integridad, y diccionario de datos.
17	¿Cuál es la probabilidad de que no se cuenten con manuales técnicos informáticos, de instalación y configuración, así como de usuario y no sean difundidos, publicados y actualizados de forma permanente?	Realizar procesos de mantenimiento preventivo y correctivo de la Infraestructura de TIC.i) Revisar e implementar un Plan de Mantenimiento preventivo y correctivo de equipo informático.
18	¿Cuál es la probabilidad de que la planificación de adquisición de software aplicativo no se alinee con los requerimientos institucionales en materia de portafolio de proyectos y servicios priorizados en los planes estratégicos, y que no cuente con la respectiva justificación técnica y autorización?	Rediseñar y alinear los servicios informáticos a las políticas y necesidades de crecimiento institucional. i) Disponer de Portafolio de servicios de la Dirección de Desarrollo Informático definido.
19	¿Cuál es la probabilidad que se desarrolle software aplicativo sin ajustarse a políticas, metodologías y estándares internacionales y no se ajuste a los requerimientos funcionales y técnicos de la institución, además, de no considerar el análisis de costo-beneficio?	Rediseñar y alinear los servicios informáticos a las políticas y necesidades de crecimiento institucional. Elaborar un Manual de Gestión de Proyectos de TIC.
20	¿Cuál es la probabilidad de no contar con un plan de adquisición de infraestructura tecnológica debidamente presupuestada y alineada a los objetivos institucionales?	Mejorar y adecuar los sistemas informáticos existentes de acuerdo a las nuevas necesidades institucionales. Revisar y mejorar los lineamientos, procedimientos, y metodología para el desarrollo, mantenimiento y/o adquisición de software.

21	¿Cuál es la probabilidad de no contar con procedimientos formalizados que garanticen el uso y mantenimiento adecuado de la infraestructura tecnológica que incluye procesos, sistemas y bitácora de las modificaciones realizadas?	Elaborar las normativas necesarias para el funcionamiento seguro y con calidad de la DDI. i) Elaborar el Manual de Procedimientos de la DDI para una adecuada operación de los servicios informáticos. ii). Elaborar un Manual de Gestión de Proyectos de TIC. iii) Reglamento de responsabilidad y uso de la firma electrónica.
22	¿Cuál es la probabilidad de no contar con manuales técnicos y de usuarios, actualizados y difundidos necesarios en cada cambio o mantenimiento de sistemas informáticos e infraestructura?	Elaborar las normativas necesarias para el funcionamiento seguro y con calidad de la DDI. i) Elaborar el Manual de Procedimientos de la DDI para una adecuada operación de los servicios informáticos. ii). Elaborar un Manual de Gestión de Proyectos de TIC. iii) Reglamento de responsabilidad y uso de la firma electrónica.
23	¿Cuál es la probabilidad de no contar con ambientes independientes adecuados para pruebas de nuevos sistemas de información e infraestructura que garantizar la integridad, disponibilidad, confiabilidad y seguridad de la infraestructura de tecnología de información disponible?	Fortalecer el Centro de Desarrollo de Software. i) Revisar y mejorar los lineamientos, procedimientos, y metodología para el desarrollo, mantenimiento y/o adquisición de software. ii) Elaborar el Modelo de Datos de la Universidad de Cuenca que incluya las reglas de validación, control, integridad, y diccionario de datos.
24	¿Cuál es la probabilidad de no contar con un plan de mantenimiento preventivo y correctivo formalizado que incluya programación de revisiones periódicas y monitoreo, necesidades organizacionales, evaluación de vulnerabilidades y requerimientos de seguridad?	Implementar proceso de mejora continua en la prestación de los servicios informáticos. i) Se dispone de un Sistema de control de acceso y seguridad física de la DDI. ii) Elaborar un Procedimiento de creación y baja de usuarios de los sistemas y servicios informáticos. iii) Disponer de un repositorio de documentos técnicos de la DDI que faciliten la gestión y operación de las TIC. Revisar e implementar un Plan de Mantenimiento preventivo y correctivo de equipo informático.
25	¿Cuál es la probabilidad de no contar con políticas, mecanismos o procedimientos que protejan y salvaguarden contra pérdidas, fugas: los medios físicos y de la información que se procesa a través de los sistemas informáticos, que incluyan mecanismos de detección y bloqueo de intrusos externos e internos , suplantación de identidades, así como políticas para ser parte de redes o grupos de seguridad informática para tratamiento de incidentes que eviten daños de los sistemas informáticos institucionales ?	Elaborar las normativas necesarias para el funcionamiento seguro y con calidad de la DDI. i) Elaborar el Manual de Procedimientos de la DDI para una adecuada operación de los servicios informáticos. ii) Elaborar un Manual de Gestión de Proyectos de TIC. iii. Reglamento de responsabilidad y uso de la firma electrónica. Implementar un Sistema de Gestión de Incidentes de seguridad (CSIRT) de las TIC.
26	¿Cuál es la probabilidad de no contar con una ubicación adecuada y un control del acceso físico para la unidad de tecnología de información y en especial a las áreas de: servidores, desarrollo y demás áreas tecnológicas sensibles?	Implementar proceso de mejora continua en la prestación de los servicios informáticos. i) Disponer de un Sistema de control de acceso y seguridad física de la DDI.
27	¿Cuál es la probabilidad de no contar con un procedimiento formalizado de obtención periódica de respaldos de información crítica o sensible, donde se especifique un cronograma y lugares de almacenamiento externos a la institución?	Elaborar las normativas necesarias para el funcionamiento seguro y con calidad de la DDI. i) Elaborar el Manual de Procedimientos de la DDI para una adecuada operación de los servicios informáticos. ii). Elaborar un Manual de Gestión de Proyectos de TIC. iii) Reglamento de responsabilidad y uso de la firma electrónica. Disponer de un Procedimiento de respaldos de información de servidores centrales en donde se especifique cronograma, custodios, lugares de almacenamiento externo.
28	¿Cuál es la probabilidad de no contar con un sistema de administración de reportes de incidentes de seguridad en el que se considere registro y reporte de incidentes y acciones correctivas?	Elaborar las normativas necesarias para el funcionamiento seguro y con calidad de la DDI. i) Elaborar el Manual de Procedimientos de la DDI para una adecuada operación de los servicios informáticos. ii) Elaborar un Manual de Gestión de Proyectos de TIC. iii. Reglamento de responsabilidad y uso de la firma electrónica. Implementar un Sistema de Gestión de Incidentes de seguridad (CSIRT) de las TIC.
29	¿Cuál es la probabilidad de no contar con instalaciones físicas adecuadas para el funcionamiento del equipo de centros de datos, que incluya monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa, disponer de energía acondicionada estabilizada y polarizada?	Implementar proceso de mejora continua en la prestación de los servicios informáticos. i) Se dispone de un Sistema de control de acceso y seguridad física de la DDI. ii) Elaborar un Procedimiento de creación y baja de usuarios de los sistemas y servicios informáticos. iii) Disponer de un repositorio de documentos técnicos de la DDI que faciliten la gestión y operación de las TIC.
30	¿Cuál es la probabilidad de no disponer de sitios de procesamiento de datos, alternativos?	Implementar proceso de mejora continua en la prestación de los servicios informáticos. i) Se dispone de un Sistema de control de acceso y seguridad física de la DDI. ii) Elaborar un Procedimiento de creación y baja de usuarios de los sistemas y servicios informáticos. iii) Disponer de un repositorio de documentos técnicos de la DDI que faciliten la gestión y operación de las TIC.

31	¿Cuál es la probabilidad de no contar con políticas, mecanismos o procedimientos de seguridad informática y seguridad en la infraestructura tecnológica que incluya horarios de trabajo no convencionales?	Elaborar las normativas necesarias para el funcionamiento seguro y con calidad de la DDI. i) Elaborar el Manual de Procedimientos de la DDI para una adecuada operación de los servicios informáticos. ii) Elaborar un Manual de Gestión de Proyectos de TIC. iii. Reglamento de responsabilidad y uso de la firma electrónica
32	¿Cuál es la probabilidad de no contar con un plan de contingencias definido, aprobado e implementado formalmente que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado?	Implementar procedimientos y actividades para una adecuada operación de los servicios informáticos. i) Dispone de un Procedimiento de respaldos de información de servidores centrales en donde se especifique cronograma, custodios, lugares de almacenamiento externo. ii) Implementar un Sistema de Gestión de Incidentes de seguridad (CSIRT) de las TIC. iii) Implementar el Plan de Gestión de Riesgos de la DDI. Elaborar un Plan de Contingencias de las TIC
33	¿Cuál es la probabilidad de no contar con un plan de gestión de riesgos que incluya la definición y asignación de roles críticos para administrar los riesgos de tecnología de información, escenarios de contingencias, la responsabilidad específica de la seguridad de la información, la seguridad física y su cumplimiento?	Implementar procedimientos y actividades para una adecuada operación de los servicios informáticos. i) Dispone de un Procedimiento de respaldos de información de servidores centrales en donde se especifique cronograma, custodios, lugares de almacenamiento externo. ii) Implementar un Sistema de Gestión de Incidentes de seguridad (CSIRT) de las TIC. iii) Implementar el Plan de Gestión de Riesgos de la DDI
34	¿Cuál es la probabilidad de no contar con un plan de continuidad de las TIC?	Elaborar un Plan de Contingencias de las TIC. i) Elaborar un Plan de Contingencias de las TIC.
35	¿Cuál es la probabilidad de no contar con un plan de recuperación de desastres formalmente definido y adecuado que contenga las actividades previas al desastre (bitácora de operaciones), las actividades durante el desastre (plan de emergencias, entrenamiento) y las actividades después del desastre?	Elaborar un Plan de Contingencias de las TIC. i) Elaborar un Plan de Contingencias de las TIC.
36	¿Cuál es la probabilidad de no contar con procedimientos legalizados y difundidos de operación del soporte tecnológico que garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen?	Elaborar un Plan de Contingencias de las TIC. i) Elaborar un Plan de Contingencias de las TIC.
37	¿Cuál es la probabilidad de no contar con un procedimiento formalizado de obtención periódica de respaldos de librerías de software y recuperación de datos?	Elaborar un Plan de Contingencias de las TIC. i) Elaborar un Plan de Contingencias de las TIC.
38	¿Cuál es la probabilidad de no contar con mecanismos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico, entrega de información y de mensajes sensitivos, así como la protección y conservación de información utilizada para encriptación y autenticación?	Definir Políticas de Tecnologías de Información y Comunicaciones (TIC) de la Universidad de Cuenca i) Elaborar un documento de Políticas de Seguridad de las TIC.
39	¿Cuál es la probabilidad de no contar con revisiones periódicas y el seguimiento requerido para determinar si la capacidad y desempeño actual y futura de los recursos tecnológicos son suficientes para cubrir los niveles de servicio acordados con los usuarios?	Elaborar un Plan Anual de Adquisición de Infraestructura de TIC.
40	¿Cuál es la probabilidad de no tener un control adecuado de los roles y usuarios para acceso al sistema de información institucional que avalen y operativicen la identificación, autenticación y autorización de los usuarios, así como la administración de las cuentas?	Implementar proceso de mejora continua en la prestación de los servicios informáticos. i) Se dispone de un Sistema de control de acceso y seguridad física de la DDI. ii) Elaborar un Procedimiento de creación y baja de usuarios de los sistemas y servicios informáticos. iii) Disponer de un repositorio de documentos técnicos de la DDI que faciliten la gestión y operación de las TIC. Elaborar un documento de Políticas de Seguridad de las TIC.

41	¿Cuál es la probabilidad de no contar con medidas de prevención, detección y corrección debidamente legalizadas que apoyen en la protección a los sistemas de información y a la tecnología de la organización de software malicioso y virus informáticos?	Implementar procedimientos y actividades para una adecuada operación de los servicios y sistemas informáticos. i) implementar un Sistema de Gestión de Incidentes de seguridad de las TIC.
42	¿Cuál es la probabilidad de no contar con una definición de los procesos claves de las TIC alineados a los requerimientos y prioridades institucionales?	Rediseñar y alinear los servicios informáticos a las políticas y necesidades de crecimiento institucional.
43	¿Cuál es la probabilidad de no contar con un repositorio de documentos técnicos, diagramas y configuraciones de hardware y software actualizado que garantice su integridad, disponibilidad y faciliten la resolución de requerimientos de TIC?	Implementar procedimientos y actividades para una adecuada operación de los servicios y sistemas informáticos. i) implementar un Sistema de Gestión de Incidentes de seguridad de las TIC.
44	¿Cuál es la probabilidad de no contar con un sistema de gestión de TIC que incluya monitoreo de la contribución, e impacto, indicadores de métrica y proceso, satisfacción de clientes, cronograma de entrega de informes de gestión y acciones correctivas plateadas por las autoridades?	Implementar proceso de mejora continua en la prestación de los servicios informáticos. i) Se dispone de un Sistema de control de acceso y seguridad física de la DDI. ii) Elaborar un Procedimiento de creación y baja de usuarios de los sistemas y servicios informáticos. iii) Disponer de un repositorio de documentos técnicos de la DDI que faciliten la gestión y operación de las TIC.
45	¿Cuál es la probabilidad de que en el plan de comunicación no se incluyan aspectos relacionados con administración de sitios Web y servicios de internet e intranet?	Elaborar e implementar un plan de cobertura de Internet.
46	¿Cuál es la probabilidad de no contar con un plan de capacitación informática especializada al personal de tecnología de usuarios desarrollado en coordinación con la unidad de talento humano y está debidamente legalizada y presupuestada?	Implementar proceso de mejora continua en la prestación de los servicios informáticos. i) Se dispone de un Sistema de control de acceso y seguridad física de la DDI.
47	¿Cuál es la probabilidad de no contar la realización de auditoria de los mensajes firmados electrónicamente y procesos automatizados de validación de certificados de firma electrónica?	Implementar proceso de mejora continua en la prestación de los servicios informáticos. i) Se dispone de un Sistema de control de acceso y seguridad física de la DDI. ii) Elaborar un Procedimiento de creación y baja de usuarios de los sistemas y servicios informáticos. iii) Disponer de un repositorio de documentos técnicos de la DDI que faciliten la gestión y operación de las TIC. Disponer del reglamento de responsabilidad y uso de la firma electrónica.
48	¿Cuál es la probabilidad de no contar con procedimientos que permitan respaldar y almacenar bajo su responsabilidad en su estado original, los archivos electrónicos o mensajes de datos firmados electrónicamente, a través de medios electrónicos seguros?	Implementar proceso de mejora continua en la prestación de los servicios informáticos. i) Se dispone de un Sistema de control de acceso y seguridad física de la DDI. ii) Elaborar un Procedimiento de creación y baja de usuarios de los sistemas y servicios informáticos. iii) Disponer de un repositorio de documentos técnicos de la DDI que faciliten la gestión y operación de las TIC. Disponer del reglamento de responsabilidad y uso de la firma electrónica.
49	¿Cuál es la probabilidad de no contar con procedimientos que regulen el uso y responsabilidad del titular de la firma electrónica?	Implementar proceso de mejora continua en la prestación de los servicios informáticos. i) Se dispone de un Sistema de control de acceso y seguridad física de la DDI. ii) Elaborar un Procedimiento de creación y baja de usuarios de los sistemas y servicios informáticos. iii) Disponer de un repositorio de documentos técnicos de la DDI que faciliten la gestión y operación de las TIC. Disponer del reglamento de responsabilidad y uso de la firma electrónica

Fuente: Tomado del Plan de Mitigación de Riesgos Académicos y Administrativos de la Universidad de Cuenca, CÓDIGO: DIP-UC-004 con fecha 08/10/2012

Anexo 2: Mapeo Metas Corporativas y Metas de TI.

Metas relacionadas con TI			Metas Corporativas																
			1. Valor para las partes interesadas de las inversiones de Negoci	2. Cartera de productos y servicios competitivos	3. Riesgos de negocio gestionados (salvaguarda de activos)	4. Cumplimiento de Leyes y regulaciones externas	5. Transparencia financiera	6. Cultura de servicio orientada al cliente	7. Continuidad y disponibilidad del servicio de negocio	8. Respuestas ágiles a un entorno de negocio cambiante	9. Toma estratégica de decisiones basada en información	10. Optimización de costes de entrega del servicio	11. Optimización de la funcionalidad de los procesos de negoci	12. Optimización de los costes de los procesos de negocio	13. Programas gestionados de cambio en el negocio	14. Productividad operacional y de los empleados	15. Cumplimiento con las políticas internas	16. Personas preparadas y motivadas	17. Cultura de innovación de producto negocio
Financiera	1	Alineamiento de TI y estrategia del negocio	P	P	S			P	S	P	P	S	P	S	P			S	S
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio, de las leyes y regulaciones externas			S	P											P		
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S					S	S		S		P			S	S
	4	Riesgos de negocio relacionados con las TI gestionados			P	S			P	S		P			S		S	S	
	5	Realización de beneficios portafolio inversiones y servicios relacionados con TI	P	P				S		S		S	S	P		S			S
	6	Transparencia de los costes, beneficios y riesgos de la TI	S		S		P				S	P		P					
Cliente	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Interno	9	Agilidad de las TI	S	P	S			S		P			P		S	S		S	P
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones			P	P			P								P		
	11	Optimización de activos, recursos y capacidades de la TI	P	S						S		P	S	P	S	S			S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones en procesos	S	P	S			S		S		S	P	S	S	S			S
	13	Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y	P	S	S			S				S		S	P				
	14	Disponibilidad de información útil y relevante para la toma de decisiones	S	S	S	S			P		P		S						
	15	Cumplimiento de TI con las políticas internas			S	S											P		
Aprendizaje y crecimiento	16	Personal del negocio y de las TI competente y motivado	S	S	P			S		S						P		P	S
	17	Conocimiento, experiencia e iniciativas para la innovación del negocio	S	P				S		P	S		S		S			S	P

Fuente: (ISACA, 2012)

Anexo 3: Mapeo entre las Metas Relacionadas con las TI de COBIT 5 y los Procesos.

			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
			Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio las leyes y las regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con TI	Transparencia de los costes, beneficios y riesgos de TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la Información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
Procesos de COBIT 5			Financiera						Cliente		Interna							A y C	
Evaluar, Orientar y Supervisar	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno.	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	Asegurar la Entrega de Beneficios	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	Asegurar la Optimización del Riesgo	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Asegurar la Optimización de los Recursos	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	Asegurar la Transparencia hacia las partes interesadas	S	S	P			P	P						S	S	S		S
Alinear, Planificar y Organizar	APO01	Gestionar el Marco de Gestión de TI	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO02	Gestionar la Estrategia	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	Gestionar la Arquitectura Empresarial	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO04	Gestionar la Innovación	S			S	P			P	P		P	S		S			P
	APO05	Gestionar el Portafolio	P		S	S	P	S	S	S	S		S		P				S
	APO06	Gestionar el Presupuesto y los Costes	S		S	S	P	P	S	S			S		S				
	APO07	Gestionar los Recursos Humanos	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	Gestionar las Relaciones	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	Gestionar los Acuerdos de Servicio	S			S	S	S	P	S	S	S	S		S	P	S		
	APO10	Gestionar los Proveedores		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO11	Gestionar los Calidad	S	S		S	P		P	S	S		S		P	S	S	S	S
	APO12	Gestionar el Riesgo		P		P		P	S	S	S	P			P	S	S	S	S
	APO13	Gestionar la Seguridad		P		P		P	S	S		P				P			
Construcción, Adquisición e Implementación	BAI01	Gestionar los Programas y Proyectos	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Gestionar la Definición de Requisitos	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Gestionar la Identificación y Construcción de Soluciones	S			S	S		P	S			S	S	S	S			S
	BAI04	Gestionar la Disponibilidad y la Capacidad				S	S		P	S	S		P		S	P			S
	BAI05	Gestionar la Introducción de Cambios Organizativos	S		S		S		S	P	S		S	S	P				P
	BAI06	Gestionar los Cambios			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Gestionar la Aceptación del Cambio y de la Transición				S	S		S	P	S			P	S	S	S		S
	BAI08	Gestionar el Conocimiento	S				S		S	S	P	S	S			S		S	P
	BAI09	Gestionar los Activos		S		S		P	S		S	S	P			S	S		
	BAI10	Gestionar la Configuración		P		S		S		S	S	S	P			P	S		
Entregar, Dar	DSS01	Gestionar las Operaciones		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Gestionar las Peticiones e Incidentes del Servicio				P			P	S		S				S	S		S
	DSS03	Gestionar los Problemas		S		P	S		P	S	S		P	S		P	S		S
	DSS04	Gestionar la Comunidad	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	Gestionar los Servicios de Seguridad	S	P		P			S	S		P	S	S		S	S		
	DSS06	Gestionar los Controles de los Procesos del Negocio		S		P			P	S		S	S	S		S	S	S	S
S, E , Val.	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno		P		P		S	S	S		S				S	P		S
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos		P		P	S		S			S					S		S

Fuente: (ISACA, 2012)

DENOMINACIÓN	PROCESOS	PRÁCTICA CLAVE DE GOBIERNO	OBJETIVOS				NORMATIVA																RESUMEN		
			1.Fortalecer la estructura organizacional	2. Automatizar los procesos de la universidad	3. Mejorar progresivamente la prestación de	4. Mejorar las estructuras de TI	Organización Informática	Segregación de Funciones	Plan informático Estratégico de tecnología	Políticas y procedimientos	Modelo de formación organizacional	Administración de proyectos tecnológicos	Desarrollo y adquisición de software aplicativo	Adquisiciones de infraestructura tecnológica	Mantenimiento y control de la infraestructura TI	Seguridad de la TI	Plan de contingencias	Administración de Soporte de TI	Monitoreo y evaluación de procesos y servicios	Sitio web, servicio de internet e intranet	Capacitación Informática	Comité informático	Firmas	OBJETIVO	NORMA	RIESGO
ALINEAR, PLANIFICAR Y ORGANIZAR	APO 01 Gestionar el marco de gestión de TI	.01 Definir la estructura organizativa					■															■				x	S
		.02 Establecer roles y responsabilidades				■		■																	x	S
		.03 Mantener los elementos catalizadores del sistema de gestión	■							■										■				x	x	P
		.04 Comunicar los objetivos y la dirección de gestión	■																							
		.05 Optimizar la ubicación de la función de TI	■				■																	x	x	P
		.06 Definir la propiedad de la información (datos) del sistema									■														x	S
		.07 Gestionar la mejora continua de los procesos	■	■																				x		S
		.08 Mantener el cumplimiento con las políticas y procedimientos	■		■					■														x	x	P
	APO 02 Gestionar la Estrategia	.01 Comprender la dirección de la empresa																								
		.02 Evaluar el entorno, capacidades y rendimientos actuales																								
		.03 Definir el objetivo de las capacidades de TI																								
		.04 Realizar un análisis de diferencias																								
		.05 Definir el Plan Estratégico y la hoja de ruta							■				■	■											x	S
		.06 Comunicar la estrategia y la dirección de TI																								
	APO 03 Gestionar la Arquitectura Empresarial	.01 Desarrollar la visión de la arquitectura de la empresa																								
		.02 Definir la arquitectura de referencia									■														x	S
		.03 Seleccionar las oportunidades y las soluciones																								
		.04 Definir la implantación de la arquitectura							■																x	S
		.05 Proveer los servicios de arquitectura empresarial																								
	APO 04 Gestionar la innovación	.01 Crear un entorno favorable para la innovación	■			■																		x		S
		.02 Mantener un entendimiento del entorno de la empresa		■					■			■												x	x	P
		.03 Supervisar y explorar el entorno tecnológico																								
		.04 Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras																								
		.05 Recomendar iniciativas apropiadas adicionales			■																			x		S
		.06 Supervisar la implementación y el uso de la innovación			■																			x		S
	APO 05 Gestionar el Portafolio	.01 Establecer la meta del objetivo de inversión																								
		.02 Determinar la disponibilidad y las fuentes de fondos							■																x	S
		.03 Evaluar y seleccionar los programas																								
		.04 Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones							■																x	S
		.05 Mantener los portafolios																								

Anexo 4: Identificación de prácticas que permiten el cumplimiento de la normativa y logro de los Objetivos de la DTIC

Daisy Fernanda Alvarado Carpio
Laura Alexandra Zumba Morales

		.06	Gestionar la consecución de beneficios																													
	APO 06 Gestionar el Presupuesto y los Costes	.01	Gestionar la finanzas y la contabilidad																													
		.02	Priorizar la asignación de recursos																													
		.03	Crear y mantener presupuestos							■																				x	S	
		.04	Modelar y asignar costes																													
		.05	Gestionar costes																													
	APO 07 Gestionar los recursos humanos	.01	Mantener la dotación de personal suficiente y adecuado				■																							x	S	
		.02	Identificar personal clave de TI						■																					x	S	
		.03	Mantener las habilidades y competencias del personal	■	■	■																			■				x	x	P	
		.04	Evaluar el desempeño laboral de los empleados	■																												
		.05	Planificar y realizar un seguimiento del uso de los recursos humanos de TI y del negocio	■																										x		S	
		.06	Gestionar el personal contratado																													
	APO 08 Gestionar las relaciones	.01	Entender las expectativas del negocio				■																							x		S
		.02	Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio	■	■																									x		S
		.03	Gestionar las relaciones con el negocio			■																								x		S
		.04	Coordinar y comunicar			■					■																			x	x	P
		.05	Proveer datos de entrada para la mejora continua de los servicios				■																							x		S
	APO 09 Gestionar los acuerdos de servicio	.01	Identificar servicios de TI																													
		.02	Catalogar servicios basados en TI																													
		.03	Definir y preparar acuerdos de servicios																													
		.04	Supervisar o informar de los niveles de servicio																				■							x	S	
		.05	Revisar acuerdos de servicio y contratos																													
	APO 10 Gestionar los Proveedores	.01	Identificar y evaluar las relaciones y contratos con proveedores																													
		.02	Seleccionar proveedores																													
		.03	Gestionar contratos y relaciones con proveedores											■	■															x	S	
		.04	Gestionar el riesgo en el suministro																													
		.05	Supervisar el cumplimiento y el rendimiento del proveedor																				■							x	S	
	APO 11 Gestionar la calidad	.01	Establecer un sistema de gestión de la calidad								■																			x	S	
		.02	Definir y gestionar los estándares, procesos y prácticas de calidad								■																			x	S	
		.03	Enfocar la gestión de calidad en los clientes																													
		.04	Supervisar y hacer controles y revisiones de calidad										■																	x	S	
		.05	Integrar la gestión de calidad en la implementación de soluciones y la entrega de servicios																													
		.06	Mantener una mejora continua																													
	APO 12 Gestionar el riesgo	.01	Recopilar datos																													
		.02	Analizar el riesgo																													
		.03	Mantener un perfil de riesgo								■																			x	S	
		.04	Expresar el riesgo																													
		.05	Definir un portafolio de acciones para la gestión de riesgos								■																			x	S	
		.06	Responder al riesgo																	■										x	S	
	APO 13 Gestionar la seguridad	.01	Establecer y mantener un SGSI	■																■										x		S
		.02	Definir y gestionar un plan de tratamiento de riesgos de la seguridad de la información																	■											x	S
		.03	Supervisar y revisar el SGSI																													
CONSTRUIR, ADQUIRIR E	BAI 01 Gestionar los programas y proyectos	.01	Mantener un enfoque estándar para la gestión de programas y proyectos		■																									x		S
		.02	Iniciar un programa		■																									x		S
		.03	Gestionar el compromiso de las partes interesadas				■																							x		S
		.04	Desarrollar y mantener el plan de programa		■																									x		S

Daisy Fernanda Alvarado Carpio
Laura Alexandra Zumba Morales

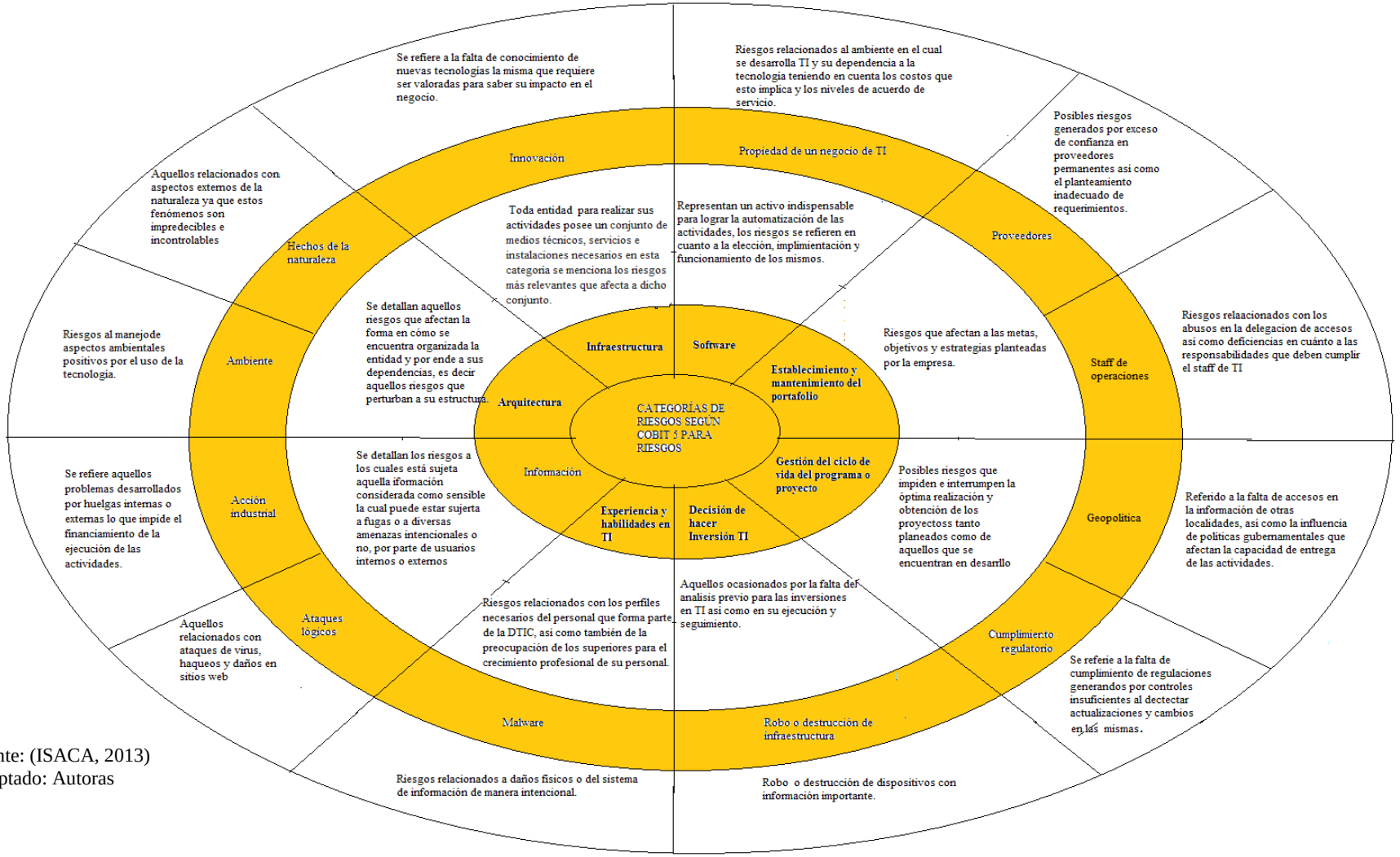
	.05	Lanzar y ejecutar el programa																							
	.06	Supervisar, controlar e informar de los resultados del programa																							
	.07	Lanzar e iniciar proyecto dentro de un programa									■												x	S
	.08	Planificar proyectos		■								■											x	x	P
	.09	Gestionar la calidad de los programas y proyectos		■																			x		S
	.10	Gestionar el riesgo de los programas y proyectos		■								■											x	x	P
	.11	Supervisar y controlar proyectos			■	■						■											x	x	P
	.12	Gestionar los recursos y los paquetes de trabajo del proyecto																							
	.13	Cerrar un proyecto		■								■											x	x	P
	.14	Cerrar un programa		■																			x		S
BAI 02 Gestionar la definición de requisitos	**.01**	Definir y mantener los requerimientos técnicos y funcionales del negocio		■									■										x	x	P
	.02	Realizar un estudio de viabilidad y proponer soluciones alternativas		■									■										x	x	P
	.03	Gestionar los riesgos de los requerimientos			■																		x		S
	.04	Obtener la aprobación de los requerimientos y soluciones				■							■										x	x	P
BAI 03 Gestionar la Identificación y Construcción de Soluciones	**.01**	Diseñar soluciones de alto nivel											■											x	S
	.02	Diseñar los componentes detallados de la solución											■											x	S
	.03	Desarrollar los componentes de la solución											■		■									x	S
	.04	Obtener los componentes de la solución											■											x	S
	.05	Construir soluciones											■											x	S
	.06	Realizar controles de calidad											■											x	S
	.07	Preparar pruebas de solución											■											x	S
	.08	Ejecutar pruebas de solución											■											x	S
	.09	Gestionar cambios de los requerimientos											■											x	S
	.10	Mantener soluciones											■											x	S
	.11	Definir los servicios de TI y mantener el catálogo de servicios											■											x	S
BAI 04 Gestionar la disponibilidad y capacidad	**.01**	Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia			■																		x		S
	.02	Evaluar el impacto en el negocio		■																			x		S
	.03	Planificar requisitos de servicio nuevos o modificados				■																	x		S
	.04	Supervisar y revisar la disponibilidad y la capacidad			■																		x		S
	.05	Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad			■																		x		S
BAI 05 Gestionar la Facilitación del Cambio Organizativo	**.01**	Establecer el deseo de cambiar																							
	.02	Formar un equipo de implementación efectivo																							
	.03	Comunicar la visión deseada																							
	.04	Facultar a los que juegan algún papel e identificar ganancias en el corto plazo																							
	.05	Facilitar la operación y el uso																							
	.06	Integrar nuevos enfoques																							
	.07	Mantener los cambios																							
BAI 06 Gestionar los cambios	**.01**	Evaluar, priorizar y autorizar peticiones de cambio		■	■							■			■								x	x	P
	.02	Gestionar cambios de emergencia				■																	x		S
	.03	Hacer seguimiento e informar de cambios de estado			■																		x		S
	.04	Cerrar y documentar los cambios				■																	x		S
BAI 07 Gestionar la Aceptación del Cambio	**.01**	Establecer un plan de implementación											■											x	S
	.02	Planificar la conversión de procesos de negocio, sistemas y datos																							
	.03	Planificar pruebas de aceptación											■											x	S
	.04	Establecer un entorno de pruebas																							
	.05	Ejecutar pruebas de aceptación											■											x	S
	.06	Pasar a producción y gestionar los lanzamientos																							

		.07 Proporcionar soporte en producción desde el primer momento																								
		.08 Ejecutar una revisión post-implementación											■												x	S
	BAI 08 Gestionar el conocimiento	**.01** Cultivar y facilitar una cultura de intercambio de conocimientos																								
		.02 Identificar y clasificar las fuentes de información																								
		.03 Organizar y contextualizar la información, transformándola en conocimiento																								
		.04 Utilizar y compartir el conocimiento																			■				x	S
		.05 Evaluar y retirar información																								
	BAI 09 Gestionar los activos	**.01** Identificar y registrar activos actuales													■										x	S
		.02 Gestionar activos críticos													■	■									x	S
		.03 Gestionar el ciclo de vida de los activos												■											x	S
		.04 Optimizar el coste de los activos																								
		.05 Administrar licencias																								
	BAI 10 Gestionar la configuración	**.01** Establecer y mantener un modelo de configuración									■														x	S
		.02 Establecer y mantener un repositorio de configuración y una base de referencia																								
		.03 Mantener y controlar los elementos de configuración																								
		.04 Generar informes de estado y configuración																								
		.05 Verificar y revisar la integridad del repositorio de configuración.																								
ENTREGAR, DAR SERVICIO Y SOPORTE	**DSS 01** Gestionar las operaciones	**.01** Ejecutar procedimientos operativos		■						■					■									x	x	P
		.02 Gestionar servicios externalizados de TI			■																			x		S
		.03 Supervisar la infraestructura de TI				■									■									x	x	P
		.04 Gestionar el Entorno				■										■								x	x	P
		.05 Gestionar las instalaciones				■										■								x	x	P
	DSS 02 Gestionar Peticiones o Incidentes de Servicio	**.01** Definir esquemas de clasificación de incidentes y peticiones de servicio																								
		.02 Registrar, clasificar y priorizar peticiones e incidentes																								
		.03 Verificar, aprobar y resolver peticiones de servicios																								
		.04 Investigar, diagnosticar y localizar incidentes																								
		.05 Resolver y recuperarse de incidentes															■								x	S
		.06 Cerrar peticiones de servicio o incidentes																								
		.07 Seguir el estado y emitir informes																								
	DSS 03 Gestionar los problemas	**.01** Identificar y clasificar problemas				■																		x		S
		.02 Investigar y diagnosticar problemas			■																			x		S
		.03 Levantar errores conocidos			■																			x		S
		.04 Resolver y cerrar problemas				■																		x		S
		.05 Realizar un gestión de problemas proactiva		■	■																			x		S
	DSS 04 Gestionar la continuidad	**.01** Definir la política de continuidad del negocio, objetivos y alcance				■											■							x	x	P
		.02 Mantener una estrategia de continuidad				■																		x		
		.03 Desarrollar e implementar una respuesta a la continuidad del negocio				■																		x		
		.04 Ejecutar, probar y revisar el plan de continuidad				■																		x		
		.05 Revisar, mantener y mejorar el plan de continuidad		■													■							x	x	P
		.06 Proporcionar formación con el plan de continuidad			■																			x		
		.07 Gestionar acuerdos de respaldo			■											■								x	x	P
		.08 Ejecutar revisiones post-reanudación																								
	DSS 05 Gestionar los servicios de seguridad	**.01** Proteger contra software malicioso (malware)				■												■						x	x	P
		.02 Gestionar la seguridad de la red y las conexiones		■																			■	x	x	P
		.03 Gestionar la seguridad de los puestos de usuario final		■														■						x	x	P
		.04 Gestionar la identidad del usuario y el acceso lógico			■																			x		S
		.05 Gestionar el acceso físico a los activos de TI				■																	■	x	x	P

SUPERVISAR, EVALUAR Y VALORAR		.06	Gestionar documentos sensibles y dispositivos de salida			■																			x		S
		.07	Supervisar la infraestructura para detectar eventos relacionados con la seguridad				■																			x		S
	DSS 06 Gestionar Controles de Proceso de Negocio	.01	Alinear las actividades de control embebidas en los procesos de negocio con los objetivos corporativos																									
		.02	Controlar el procesamiento de la información																									
		.03	Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización					■											■								x	S
		.04	Gestionar errores y excepciones																									
		.05	Asegurar la trazabilidad de los eventos y responsabilidades de información																									
		.06	Asegurar los activos de información																									
	MEA 01 Supervisar, Evaluar y Valorar rendimiento y conformidad.	.01	Establecer un enfoque de la supervisión				■																			x		S
		.02	Establecer los objetivos de cumplimiento y rendimiento				■																			x		S
		.03	Recopilar y procesar los datos de cumplimiento y rendimiento		■																					x		S
		.04	Analizar e informar sobre el rendimiento			■															■					x	x	P
		.05	Asegurar la implantación de medidas correctivas		■																					x		S
	MEA 02 Supervisar, Evaluar y Valorar el sistema de control interno	.01	Supervisar el control interno				■																			x		S
		.02	Revisar la efectividad de los controles sobre los procesos de negocio				■				■															x	x	P
		.03	Realizar autoevaluación de control																									
		.04	Identificar y comunicar las deficiencias de control				■																			x		S
		.05	Garantizar que los proveedores de aseguramiento son independientes y están cualificados																									
		.06	Planificar iniciativas de aseguramiento																									
		.07	Estudiar las iniciativas de aseguramiento																									
		.08	Ejecutar las iniciativas de aseguramiento																									
	MEA 03 Supervisar, Evaluar y Valorar la Conformidad	.01	Identificar requisitos externos de cumplimiento																									
		.02	Optimizar la respuesta a requisitos externos								■																x	S
		.03	Confirmar el cumplimiento de requisitos externos																									
		.04	Obtener garantía de cumplimiento de cumplimiento de requisitos externos.																									

Fuente: (Contraloría General del Estado, 2009) (ISACA, 2012)
Análisis: Autoras

Anexo 5: Categorías de Escenarios de Riesgos



Fuente: (ISACA, 2013)
Adaptado: Autoras

Daisy Fernanda Alvarado Carpio
Laura Alexandra Zumba Morales

Anexo 6: Escenarios de Riesgos

CATEGORIA DEL ESCENARIO DE RIESGO	Tipo de Riesgo: Beneficio de TI/ Habilitación de valor	Tipo de Riesgo: Programa de TI y proyecto entregado	Tipo de Riesgo: Operaciones de Servicios de TI	N°	ESCENARIOS NEGATIVOS	P
Establecimiento y mantenimiento del portafolio	P	S	S	1	Desactualización de las políticas de TI.	
	P	S	P	2	Escasez o descoordinación de requerimientos de control con relación a los objetivos o su inoportuna ejecución.	
	P	S	S	3	No existe correlación entre los objetivos del negocio y TI. (Alineación Estratégica)	
		P	S	4	Desconocimiento de los objetivos y metas institucionales que imposibilitan el posterior análisis sobre su rendimiento.	
	P	S	S	5	Falta de seguimiento y control de las soluciones implementadas.	
	P	S	S	6	Rezagar al área de TI dentro de la estructura organizacional, sin considerar su importancia y criticidad para la consecución de objetivos.	
	S	S	P	7	Las partes interesadas no son participantes activas para la entidad.	
	S	P	S	8	Requerimientos no comunicados ni aprobados antes de su puesta en marcha.	
Gestión del ciclo de vida del programa o proyecto	S	P	S	9	Incumplimiento en la realización de proyectos ya sea por errores en la planeación de presupuestos o definición de sus requisitos, por entrega retrasada de las etapas entre otros, relacionados con la parte de la tercerización.	
	S	P	S	10	Falta de involucramiento de las partes interesadas en el ciclo de proyectos, lo que genera un incremento de costes por uso adicional de recursos si existen brechas en las especificaciones o servicios al usuario final.	
	S	P	S	11	Enfoque desactualizado de la gestión de programas y proyectos.	
	S	P	S	12	Falta de disposición de una base de datos de proyectos que hayan sido debidamente analizados antes de su aprobación conforme las necesidades y capacidades de la entidad.	
	S	P	S	13	Descuido de la documentación relacionada con los proyectos considerados en el portafolio.	
	S	S	P	14	Existencia de informes sobre avances tardíos.	
	S	P	S	15	Planificación inadecuada de los proyectos.	
	S	P	S	16	Deficiencias en la comunicación verbal o escrita adoptada durante el desarrollo del ciclo de vida de un proyecto.	
	S	S	P	17	Ausencia o ineficiencia de un plan de gestión de calidad para los entregables del proyecto.	
	S	P	S	18	Ausencia de un proceso para el análisis de riesgo de un proyecto o inefectividad del mismo.	
	S	P	S	19	Criterios claves de rendimiento del proyecto no definidos claramente.	
	S	P	S	20	Falta de disposición de un proceso para el control de cambios en los proyectos.	
	S	P	S	21	Desconocimiento de las condiciones de aceptación de terceras partes.	
	S	P	S	22	Deficiencias en la presentación de las declaraciones del alcance del proyecto.	
	P	S	S	23	Falta de entendimiento de los criterios de desempeño o ausencia de los mismos.	
	S	P	S	24	Falta de claridad en los pasos claves para cerrar un proyecto.	
	P	P	S	25	Desviaciones del rendimiento de los proyectos frente a los requerimientos iniciales y ausencia de un análisis posterior.	
	S	P	S	26	Falta de formalidad en cualquier cambio de los programas.	
	P	S	S	27	Degradación de la imagen de la entidad por su incapacidad para responder oportuna y asertivamente contra incidentes que afectan a los servicios entregados por proyectos ineficientes.	
	S	P	P	28	Ausencia de supervisión y monitoreo durante el ciclo de vida del presupuesto generado y aprobado, para cada programa o proyecto.	
		P		29	Fallas en la recepción de sugerencias respecto de las acciones correctivas para los programas y proyectos.	
		P	S	30	Requerimientos que no cubren la definición de necesidades así como factibilidad económica y tecnológica.	
	P	S	S	31	Actividades incompletas sin identificar y comunicar.	
Decisión de hacer Inversión TI	S	P	S	32	Descoordinación en las inversiones importantes relacionadas con TI debido a la falta de comunicación con la alta dirección de la institución, lo que imposibilita el cumplimiento de los objetivos estratégicos planteados.	
	P	S	S	33	No se identifican, priorizan y analizan los requerimientos antes de la adquisición o desarrollo de software.	
	P	P	P	34	Selección errónea de software o infraestructura al no llevar a cabo un análisis de sus costos, viabilidad, rentabilidad y entre otros.	
	P	S	P	35	Transferencias y acuerdos de niveles de servicio con terceras partes deficientes.	
	P	S	S	36	Intercambio de información inoportuna e insuficiente con las partes interesadas.	

	S	P	S	37	Subutilización de los recursos asignados para inversión y operaciones.	
	P	S	S	38	Escasez de soluciones innovadoras que limitan la generación de valor para la empresa.	
		P		39	Inexistencia de planes alternativos en caso de que los proyectos no se puedan ejecutar o presenten inconvenientes.	
	P	S	P	40	Presupuestos no reflejan las prioridades de inversión en TI.	
Experiencia y habilidades en TI	P		S	41	Política de talento humano carente de los procedimientos y requisitos para la selección y evaluación del personal de TI.	
	P		S	42	Alta dependencia del personal clave de TI debido al exceso de confianza depositado en el mismo lo que provoca falta de rotación y compartición de tareas.	
	S		P	43	Inexistencia de métodos para la evaluación del personal.	
	S	S	P	44	Mala definición de la matriz de habilidades y competencias.	
	S	S	P	45	Ausencia de planes de desarrollo-mejora de habilidades y competencias del personal de TI lo que provoca brechas en las habilidades que poseen estos respecto a las nuevas tecnologías o métodos. (INTERNO)	
	S	S	P	46	Inconsistencias en la evaluación del desempeño por inadecuada aplicación o selección de método de evaluación.	
	S	S	P	47	Falta de inventario respecto del talento humano que forma parte del negocio y de TI.	
	S	S	P	48	Fallas en el registro de utilización de los recursos.	
	P	S	P	49	El área de TI no cumple con funciones de asesoría y apoyo a la alta dirección así como usuarios en general.	
	S	S	P	50	Errores en el manejo de procesos e información debido a un personal desinformado o poco preparado.	
	S	S	P	51	No se encuentran claramente definidas las habilidades y competencias necesarias para ocupar un puesto en TI.	
	P	S	S	52	No se brinda al personal la oportunidad de mantener y desarrollar habilidades y competencias que ayuden al cumplimiento de las metas empresariales. (EXTERNO)	
	P	S	S	53	Falta de independencia del área de TI.	
	S	S	P	54	Falta de conocimiento y entendimiento del negocio incluidas las políticas relacionadas a TI afectando la calidad de los servicios entregados.	
	P		P	55	Falta de inversión en profesionales para el área debido al exceso desconfianza en el personal de TI.	
	P	S	S	56	Falta de concientización y participación del personal en acciones preventivas que se direccionen a evitar los riesgos de salud y seguridad en el trabajo.	
	S	S	P	57	No se efectúa un análisis de los requerimientos necesarios y disponibles para tratar brechas respecto del personal.	
Información (Violación de datos: daños, fuga y acceso)			P	58	Filtración de la información hacia la competencia debido al abandono del equipo de la institución.	
			P	59	La información sensible es divulgada accidentalmente debido al fracaso en seguir directrices del tratamiento de información.	
			P	60	Protección inadecuada de información sensible tanto en el archivo en diferentes medios de almacenamiento que suelen perderse así como exponerse a divulgaciones mediante email u otros medios de comunicación social usados para ataques lógicos.	
			P	61	Desvíos de información debido a la ineficiencia en los controles de los diferentes medios de seguridad.	
			P	62	Daño de los componentes de hardware de manera intencional por el personal interno, para lograr la destrucción o modificación de los datos.	
			P	63	Datos inaccesibles por daños o fallas en la base de datos.	
	S	P	P	64	Brechas de rendimiento y capacidad de los medios utilizados para el tratamiento de la información.	
			P	65	Fallas en el registro y almacenamiento de copias de respaldo.	
	S	P	S	66	Mala programación operativa.	
	P	S	S	67	Ausencia de políticas de seguridad que establezca los intervalos para el mantenimiento de los equipamentos.	
	S	S	P	68	Falta de un plan de continuidad que imposibilita responder a incidentes e interrupciones de servicios.	
			P	69	Desactualización del plan de continuidad respecto de cambios nuevos o mayores del entorno, debido a fallas o ausencias de supervisión y monitoreo.	
	S	S	P	70	Fallas en los registros de acceso.	
	S	P	P	71	Asignación ambigua de responsabilidades sobre propiedad de información así como sistemas de información (SI).	
	S	S	P	72	Ausencia de directrices para la clasificación de datos o estás son poco claras para su aplicación.	
	S	S	P	73	Ausencia de directrices para control y seguridad de datos.	
	P	S	S	74	Desconocimiento de la información que se posee debido a la desorganización de la misma.	
	S	S	P	75	Condiciones favorables para la intrusión a la información sensible.	
	P	S	P	76	No se llevan a cabo procedimientos y actividades que permitan el soporte adecuado de información susceptible a riesgos.	
			P	77	Desconocimiento de los criterios de información en los cuales debe basarse la información convincente.	

Daisy Fernanda Alvarado Carpio
Laura Alexandra Zumba Morales

	S		P	78	Falta de procedimientos para el acceso a locales, edificios y demás instalaciones de TI.	
	S	S	P	79	Desconocimiento de políticas de seguridad en la conectividad.	
Arquitectura	P		P	80	La arquitectura de la institución no es la apropiada para apoyar los propósitos y prioridades del negocio.	
			P	81	Fallas en el plan de mitigación debido a una arquitectura compleja e inflexible lo cual provoca pérdidas en las oportunidades de negocio.	
	P	S		82	Escasez en la disponibilidad de los recursos (infraestructura, software, etc.) que imposibilita la ejecución efectiva del plan de mitigación.	
	P	P	S	83	Aplicación de un modelo que no facilita la creación, compartición y uso de la información generada en la institución.	
	S	S	P	84	Existencia de dudas por parte del usuario sobre la arquitectura de procesos e información.	
	S	S	P	85	Dificultades para la incorporación de nuevas aplicaciones y procesos de manera oportuna y efectiva.	
	P	S	S	86	Ausencia de alineación de las prácticas manejadas en el área de TI con estándares internacionales y códigos de gobierno.	
	S	S	P	87	No se considere necesaria la realización de un plan de migración e implementación.	
Infraestructura (hardware, sistema operativo y la tecnología de control) (selección / implementación, operación y desmantelamiento)	S	S	P	88	Los sistemas no se adaptan fácilmente a la creciente generación de información y cambios en los procesos relacionados.	
			P	89	Uso obsoleto de la infraestructura lo que genera insatisfacción en el cumplimiento de los nuevos requisitos empresariales (redes, seguridad, base de datos, almacenamiento)	
	P	S	S	90	Inadecuada interpretación de los impactos de eventos relacionados con la infraestructura (disponibilidad, rendimiento y capacidad) sobre la institución.	
	S	S	P	91	Identificación incorrecta de desviaciones respecto a las líneas de referencia.	
	P	S	S	92	Fallas en la divulgación o concientización de las políticas relacionadas a TI.	
	S	S	P	93	Fallas en los registros y definición de acceso a los activos físicos de TI o el uso de dispositivos por parte del usuario para tratamiento de la información.	
Software	P	P		94	No se prioriza las peticiones de cambio debido a la inexistencia de la formalidad de las mismas dentro del proceso de gestión lo cual imposibilita su evaluación y determinación del impacto en los procesos de negocio y los servicios de TI.	
		P		95	Los procesos de marcha atrás y de recuperación no son identificados y documentados de manera correcta.	
	P	S		96	Inexistencia de un plan de implementación de software que refleje la estrategia global de su ejecución.	
	S	P	P	97	Falencias en el plan de pruebas lo cual ocasiona que no se refleje claramente la evaluación de riesgos del proyecto.	
	S	P		98	Falta de procedimientos de identificación, evaluación e información que deben generar las revisiones post-implantación.	
	S	S	P	99	Los cambios aprobados no son comunicados oportunamente a los actores y usuarios relacionados.	
	S		P	100	Desconocimiento del impacto de las peticiones de cambio.	
	S	S	P	101	Falta de revisión de cambios de emergencia tras su implementación.	
	S	S	P	102	Falta de documentación de los cambios.	
		P	S	103	Imprecisión de la redacción de especificaciones lo cual provoca vacíos que influyen en las operaciones de los usuarios.	
	P	S	P	104	Ejecución de cambios sin considerar el impacto en los proveedores de servicios contratados.	
	S	P	P	105	Demora en la aprobación de cambios.	
	S	P		106	Los cambios no son registrados, analizados, priorizados, evaluados y aprobados antes de su implementación.	
		P		107	Ausencia de un plan que guíe los procesos de implementación de software.	
		P		108	Las nuevas soluciones no puedan ser totalmente operativas por ejemplo por compatibilidad.	
		P	S	109	No se maneja un plan de pruebas de aceptación en el cual participen usuarios claves.	
		P	P	110	No se establece íntegramente los recursos necesarios para ejecutar pruebas y evaluarlas al finalizar.	
		P	P	111	No se registran ni evalúan los resultados de las pruebas de: desempeño, aceptación, compatibilidad o configuración del software antes de ser oficialmente implantado.	
	S	P	S	112	No se realiza ni se da a conocer a las partes los resultados de las revisiones post-implementación.	
	P	S	S	113	No se maneja un plan de acciones correctivas y/o preventivas.	
	S	S	P	114	No se genera una BD de los usuarios de la información.	
	P		P	115	Configuración insegura de los sistemas operativos.	
			P	116	Ausencia de políticas de seguridad para dispositivos de usuario final.	
	P	S	P	117	El conocimiento no se extiende a través de la organización según corresponde a los intereses de los usuarios.	
Propiedad de un negocio de TI	P	S	S	118	Falta de establecimiento de medidas para supervisar y recolectar datos del nivel del servicio lo que imposibilita la obtención de información de las mejoras.	
	P	S	S	119	Inobservancia de los requerimientos de control de la información en los procesos de negocio, lo cual imposibilita hacer frente a los riesgos de la información y el cumplimiento de regulaciones y leyes.	
	S	P	S	120	Falta de sensibilización tanto de los objetivos de TI como de la empresa.	
	P	S	P	121	No se ejecutan procedimientos y mecanismos que permitan mejorar el nivel de satisfacción de los usuarios.	
	P	S	S	122	No hay un enfoque hacia la gestión del cumplimiento tanto para objetivos como para su rendimiento.	
	P	S	S	123	No se llevan a cabo revisiones que permitan anticipar tendencias en el rendimiento.	

Daisy Fernanda Alvarado Carpio
Laura Alexandra Zumba Morales

			P	124	Ineficiencia de los controles sobre procesos de negocio o ausencia en su aplicación.
	P	S	S	125	Inefectividad en el control de tendencias negativas por ausencia de planes.
Proveedores	P	S		126	Excesiva confianza en los proveedores con los cuales se trabaja por lo cual se carece de una BD de proveedores alternativos.
	S	S	P	127	No gestionar las relaciones con los proveedores de la institución.
	S	P	S	128	Establecimiento de procesos de comunicación con proveedores poco efectivos que impiden solucionar inconvenientes.
		P		129	Roles y responsabilidades confusas y poco definidas de las partes que intervienen en la negociación.
	P	P	S	130	No se toma en cuenta las sugerencias sobre proveedores al momento de realizar una evaluación y selección de los mismos.
	P	S	S	131	Criterios de supervisión de proveedores obsoleto, mal definidos y no operativos.
	S	S	P	132	Confianza en los proveedores permanentes lo que imposibilita la evaluación de información externa vinculada.
Cumplimiento regulatorio	P	S	P	133	Desactualización o desconocimiento de qué estándares sectoriales, códigos de buenas prácticas y guías debe adoptarse y adaptarse a la institución.
Robo o destrucción de infraestructura	S	S	P	134	Ineficiencia o ausencia de dispositivos que detectan las amenazas del entorno, debido a la falta de supervisión, mantenimiento y actualización de los mismos.
			P	135	Mantenimiento de instalaciones del área de TI efectuado por personal no autorizado incumpliendo así con las posibles recomendaciones realizadas por los proveedores.
			P	136	Libre acceso a las instalaciones de procesamiento sin peticiones formales.
			P	137	Falta de concientización y capacitación al personal sobre la seguridad de la información así como la infraestructura de soporte.
	P	S	P	138	Destrucción o descuido de la infraestructura por parte del personal responsable.
Malware	S	S	P	139	Políticas de prevención y tratamiento de software malicioso desactualizadas o ausencia de las mismas.
	S	S	P	140	Desactualización de los usuarios respecto a configuraciones de tráfico entrante, uso de correos electrónicos y descargas lo cual facilita el acceso de software malicioso (virus, gusanos, software espía y correo basura).
	S	S	P	141	Registro de incidentes de seguridad desactualizado lo que imposibilita su evaluación, investigación y retroalimentación.
	S	S	P	142	Falta de acciones de remediación después de eventos ocasionados por acción del malware.
			P	143	Procedimientos inadecuados para mantener el cumplimiento y medición del funcionamiento de los sistemas.
	S	S	P	144	Desconocimiento de los incidentes provocados por malware con datos específicos de cada uno de ellos.
	P	S	P	145	Falta de seguimiento y control de las actividades o procesos que favorecieron la ejecución del malware.
	P	S	S	146	Exposición alta a daños por ejecución de malware.
Ataques lógicos	S		P	147	Interrupción del servicio debido al ataque de denegación de servicio.
	S		P	148	La página web presenta deficiencias o alteraciones cuando existen gran cantidad de usuarios.
	P			149	Falta de claridad y operatividad de las políticas de seguridad de la información.
	S	S	P	150	Mala configuración de equipamientos de seguridad.
	P	P	P	151	Registro de eventos desactualizado.
	S	S	P	152	No se supervisa la estructura de TI y los eventos que la afecten.
	P	S	P	153	No se detallan procedimientos de revisión de eventos y retroalimentación.
	S	S	P	154	Ataques de virus, gusanos, troyanos, rootkits, spyware, etc.
Acción industrial	S	S	P	155	Inoperatividad de la entidad por el surgimiento de huelgas relacionadas con partes internas como los trabajadores o externas como proveedores.
Ambiente	S	S	P	156	El equipo utilizado no es amigable con el medio ambiente (consumo de energía eléctrica).
Hechos de la naturaleza	S	S	P	157	Inundaciones
	S	S	P	158	Temblores/Terremotos
	S	P	S	159	Ausencia de acciones que identifique la probabilidad de ocurrencia de desastres naturales.
Innovación	P	S	S	160	Fallas en la identificación de nuevas e importantes tendencias tecnológicas.
	P		S	161	Falta de adopción y explotación de nuevos software (funcionalidad, optimización) de manera oportuna.
	S	P	S	162	Ausencia de un plan de innovación o fallas en el mismo.
	P	S	S	163	Escasez de mecanismos para promover y captar ideas de los empleados.
	S	S	P	164	Falta de periodicidad en las reuniones para informar sobre la posibilidad de adopción de nuevas tecnologías y los beneficios de estas para la entidad.
		P	S	165	Ausencia de recomendaciones respecto de los resultados de las pruebas de conceptos.
	S	P	P	166	Operatividad con tecnología obsoleta.

Fuente: Autoras

Anexo 7: Formato de Encuesta

UNIVERSIDAD DE CUENCA

Encuesta a la Dirección de Tecnologías de Información y Comunicación

TEMA DE TESIS : Elaborar un Plan de Gestión de Riesgos de Sistemas de Información basado en el Marco COBIT 5 para Riesgos, el mismo que se aplicará en la Universidad de Cuenca

Tutor: Ing. Paul Ochoa, MBA,CISA
Fecha: 28 de enero del 2015
Duración:
Entrevistado:
Entrevistadoras: Daysi Fernanda Alvarado Carpio - Laura Alexandra Zumba Morales

ENUNCIADO	OPCIONES	
Mantener las habilidades y competencias del personal	**SI**	**NO**
1. Dentro de la DTIC ¿se encuentra definido un método de evaluación al personal enfocado en las habilidades y competencias necesarias para lograr los objetivos de la empresa, de esta área y procesos en general? ¿En qué consiste dicho método? ESPECIFIQUE:_____		
¿Con que frecuencia se lo aplica? Mensual _____ Trimestral_____ Semestral___ Anual _____		
2. ¿Se actualizan periódicamente los planes de acción referentes a: la formación, contratación, redistribución y los cambios en las estrategias de contratación?		
¿Con que frecuencia? Mensual _____ Trimestral_____ Semestral___ Anual _____		
3. ¿Se dispone de un Manual de funciones para el personal de TIC?		
4. ¿Se dispone de un Plan de Carrera?		
5. ¿Se cuenta con un Plan de Capacitación al personal?		
6. ¿Se encuentra definido un procedimiento para la sucesión de cargos? ESPECIFIQUE:_____		
Evaluar, priorizar y autorizar peticiones de cambio	**SI**	**NO**
1. ¿Existe un proceso de gestión de cambios dentro de DTIC?		
2. ¿Con que frecuencia se evalúan las peticiones de cambio? Quincenal___ Mensual___ Trimestral___		
3. ¿Existe una persona delegada para el análisis y seguimiento de las peticiones de cambio? ¿Quien es el responsable de esta actividad? ESPECIFIQUE:_____		
4. ¿Cómo se define el impacto de los cambios a las partes relacionadas? ESPECIFIQUE:_____		
Mantener el cumplimiento con las políticas y procedimientos	**SI**	**NO**
1. ¿Se manejan Políticas para la DTIC?		
5. ¿Existe un Código de Conducta para el personal?		
2. ¿Se da seguimiento al cumplimiento y actualización de políticas y procedimientos referentes al personal y funciones de TIC?		
¿Con que frecuencia? Mensual _____ Trimestral_____ Semestral___ Anual _____		
3. ¿Existe una persona encargada de realizar el seguimiento al cumplimiento de políticas y procedimientos establecidos, actualización así como aplicar las sanciones correspondientes? ESPECIFIQUE:_____		
4. ¿Cómo se asegura que los procedimientos definidos están siendo aplicados? ESPECIFIQUE:_____		

Proyectos	SI	NO
1.¿Se encuentra definido un portafolio de proyectos? ¿Cómo está conformado dicho portafolio? ESPECIFIQUE:_____		
2. ¿Se manejan indicadores para la evaluación de los proyectos versus los criterios de desempeño inicialmente definidos?		
¿Cuales? ESPECIFIQUE:_____		
3. ¿Se manejan informes de los progresos de los proyectos con base en lo que muestran los indicadores?		
4. ¿Se ha definido un proceso para la evaluación de desviaciones surgidas en el proyecto? ¿Quién es la persona encargada de ello? ESPECIFIQUE:_____		
5. ¿Se toman en cuenta las recomendaciones dadas respecto de los proyectos y existe una posterior supervisión de las acciones correctivas que se haya tomado, si así lo amerita el caso?		
6. ¿Se mantiene una adecuada y permanente comunicación con las partes interesadas respecto de los cambios que han surgido durante el desarrollo del proyecto?		
7. ¿Se maneja una guía o marco referencial que cubra el ciclo de vida del proyecto? ¿Cuál? ESPECIFIQUE:_____		
8. Cuando está de por medio la ejecución de múltiples proyectos ¿se determinan actividades de interdependencia, colaboración y comunicación necesarias?		
9. ¿Se determinan planes de gestión de riesgos para los diversos proyectos? ¿Cómo? ESPECIFIQUE:_____		
10. ¿Existe delegación de responsabilidades al ejecutar el proceso de gestión de riesgos?		
11. ¿Se hacen reevaluaciones periódicas de los riesgos identificados con anterioridad?		
12. ¿Existe un listado de riesgos potenciales identificados?		
13. ¿Existe un procedimiento definido para el Cierre de Proyectos?		
14. ¿Se han identificado pasos claves para el cierre de un programa o proyecto? ¿Cuáles? ESPECIFIQUE:_____		
15. ¿Existen revisiones post-implementación después de concluido un programa o proyecto? ¿En qué periodo de plazo? ESPECIFIQUE:_____		
16. ¿Existe retroalimentación en los proyectos y se toma en cuentas las recomendaciones que surgen?		
Definir y mantener los requerimientos técnicos y funcionales del negocio	**SI**	**NO**
1. ¿Se han definido requerimientos estándares, dentro de la organización para la generación de proyectos, acorde a la naturaleza del negocio?		
¿Cuáles por ejemplo? ESPECIFIQUE:_____		
2. ¿Se mantiene una comunicación continua durante el ciclo de vida de un proyecto? ¿Cuál es el proceso para ello? ESPECIFIQUE:_____		
3. Dentro de los criterios de aceptación de un proyecto ¿se consideran los controles de: información, cumplimiento legal y regulatorio, auditabilidad entre otros al momento de su definición?		
4. ¿Se realiza seguimiento de los cambios generados durante el ciclo de vida de los proyectos?		
Obtener la aprobación de los requerimientos y soluciones	**SI**	**NO**
1. ¿Se encuentra delegada una persona como responsable para la revisión y aceptación final de una solución o requerimiento?		
2. ¿Se han establecido parámetros para las revisiones de calidad?		
3. ¿En qué fases de proyecto se llevan a cabo las revisiones de calidad? ESPECIFIQUE:_____		

Realizar un estudio de viabilidad y proponer soluciones alternativas	**SI**	**NO**
1. ¿Se ejecutan estudios de viabilidad antes de la toma de decisiones?		
2. Al realizar la planificación y desarrollo de soluciones ¿se tienen en cuenta aspectos como: la arquitectura empresarial, el tiempo y el presupuesto?		
3. Para la toma de decisiones respecto a las soluciones ¿las partes interesadas son tomadas en cuenta y se les dan a conocer costes y riesgos atenientes a la solución?		
4. ¿Se manejan Informes de viabilidad sobre un proyecto de manera oportuna?		
Ejecutar procedimientos operativos	**SI**	**NO**
1. ¿Las actividades y procedimientos operativos son diseñados de manera tal que permitan dar apoyo a los servicios entregados?		
2. ¿Se generan informes de satisfacción del usuario sobre si los resultados fueron adecuados con un determinado nivel de seguridad y oportunos?		
3. ¿Se consideran estándares de seguridad para la recepción, procesamiento, almacenamiento y salida de los datos? ¿Cuáles son dichos estándares? ESPECIFIQUE:_____		
4. ¿Cuáles son los servicios que brinda DTIC? ESPECIFIQUE:_____		
5. ¿Se ha definido un procedimiento para Gestión de Usuarios?		
Ubicación de TI		
1. ¿Qué posición ocupa la DTIC dentro del Organigrama funcional de la Universidad? ESPECIFIQUE:_____		
2. ¿Se maneja un Manual de funciones de DTIC?		
Mantener un entendimiento del entorno de la empresa	**SI**	**NO**
1. Se realizan reuniones con las unidades de negocio, divisiones y/o otras entidades interesadas de manera periódica?		
¿Con que frecuencia? Mensual _____ Trimestral_____ Semestral___ Anual _____		
2. ¿Cuáles son las unidades, divisiones y demás, que están presentes para tratar el uso de nuevas tecnologías? ESPECIFIQUE:_____		
3. ¿Se ha aprobado el Plan Operativo Anual 2015 con participación de las partes interesadas?		
Coordinar y comunicar	**SI**	**NO**
1. ¿Existe coordinación y comunicación respecto de: actividades operativas, roles y responsabilidades a cada nivel, transición y demás relacionadas en toda la organización?		
2. ¿Se maneja un plan de comunicación?		
3. ¿Cómo se encuentra compuesto el plan de comunicación y quien es el encargado de su aplicación y mantenimiento? ESPECIFIQUE:_____		
Supervisar la infraestructura de TI	**SI**	**NO**
1. ¿Existe supervisión de la infraestructura de TI?		
¿Cuál es el procedimiento para ello? ESPECIFIQUE:_____		
2. ¿Se mantiene una lista de activos de TI en la cual se identifican aquellos considerados críticos de supervisar?		
3. ¿Se lleva un registro de los eventos que se han suscitado, con información suficiente que incluya riesgos y rendimiento?		
Gestionar el Entorno	**SI**	**NO**
1. ¿Se han identificados los posibles desastres naturales que pueden afectar a la infraestructura de DTIC así como el nivel de impacto de los mismos?		
2. ¿Se han establecido medidas para la protección de amenazas externas tanto de equipamento de TI como de instalaciones? ¿Cuáles son estas? ESPECIFIQUE:_____		
3. ¿Qué tipos de pólizas son utilizadas en el DTIC para aseguramiento de las instalaciones y equipos? ESPECIFIQUE:_____		

Gestionar las instalaciones	**SI**	**NO**
1. ¿Se manejan sistemas de alimentación ininterrumpida (SAI) y se asegura una dotación eléctrica adecuada y continua?		
2. ¿Se manejan protecciones alternativas? ¿Cuáles son? ESPECIFIQUE:_____		
3. ¿Se efectúa simulacros de incendios y rescate dentro de las instalaciones?		
4. ¿Se capacita al personal sobre leyes, regulaciones y directrices relacionadas a seguridad en el trabajo así como salud del trabajador?		
5. ¿Se da mantenimiento periódico a los sitios y equipamentos de TIC?		
¿Con que frecuencia se lo aplica? Mensual ____ Trimestral____ Semestral___ Anual ___		
Definir la política de continuidad del negocio, objetivos y alcance	**SI**	**NO**
1. ¿Se han identificado procesos de negocio, propios o subcontratados, que sean críticos para las operaciones del negocio?		
2. ¿Se maneja un Plan de Continuidad del Negocio?		
3. ¿Se encuentran definidas las políticas de continuidad y alcances mínimos de las mismas?		
Revisar, mantener y mejorar el plan de continuidad	**SI**	**NO**
1. ¿Se actualiza periódicamente el plan de continuidad acorde a la realidad en la cual la organización desarrolla sus actividades?		
2. ¿Se realiza un análisis de riesgos de nuevos cambios acerca de las amenazas potenciales sobre los procesos de negocio y su impacto?		
Gestionar acuerdos de respaldo	**SI**	**NO**
1. ¿Con qué frecuencia se actualizan los requerimientos para copias de seguridad?		
2. ¿Cuáles son los tipos de copias de seguridad más utilizados? ESPECIFIQUE:_____		
Proteger contra software malicioso (malware)	**SI**	**NO**
1. ¿Existen procedimientos y responsabilidades de prevención para evitar el perjuicio por algún software malicioso?		
2. ¿Se ha definido herramientas de protección contra software malicioso?		
3. ¿Existe evaluaciones de amenazas potenciales presentadas en la institución?		
4. ¿Se posee una filtración del tráfico entrante para protección de información no deseada?		
5. ¿Se conoce si los usuarios han instalado software compartido o no autorizado?		
Gestionar la seguridad de la red y las conexiones	**SI**	**NO**
1. ¿Dentro de la política de seguridad y uso de la red establecida por la institución se definen los conceptos de red interna y externa?		
2. ¿Existe requisitos para acceder a la red como los datos del equipo? Especifique. ESPECIFIQUE:_____		
3. ¿Los protocolos de seguridad son debidamente analizados previamente y aprobados, de forma que exista una lista de los mismos que permitan conocer de dicha aprobación en cualquier instante?		
Gestionar la seguridad de los puestos de usuario final	**SI**	**NO**
1. ¿Existe un punto de red por puesto de trabajo?		
2. ¿Se posee mecanismos de bloqueo de los dispositivos?		
Gestionar el acceso físico a los activos de TI	**SI**	**NO**
1. ¿Existe limitaciones para el acceso a locales, edificios y demás áreas?		
2. ¿Se lleva un registro manual o electrónico del acceso a los locales, edificios y áreas?		
Analizar e informar sobre el rendimiento	**SI**	**NO**
1. ¿La dirección da paso o acepta recomendaciones para cambios a los objetivos y métricas?		
2. ¿Cuáles son los métodos para evaluar el desempeño y cumplimiento de los objetivos? ESPECIFIQUE:_____		
Revisar la efectividad de los controles sobre los procesos de negocio	**SI**	**NO**
1. ¿Se llevan a cabo evaluaciones para evidenciar si el control interno está funcionando adecuadamente?		
2. ¿Cuáles son los mecanismos para el mantenimiento de evidencias? ESPECIFIQUE:_____		

Fuente: Autoras

Anexo 8: Riesgos levantados según encuesta

OBJETIVO	N° de Riesgo	RIESGO
Conocer si el personal de TIC tiene las competencias necesarias para desempeñar sus actividades y por parte de la organización existe intereses en mantener y mejorar las habilidades del personal a través de planes relacionados y evaluaciones pertinentes.	*43*	Inexistencia de métodos para la evaluación del personal.
	45	Ausencia de planes de desarrollo-mejora de habilidades y competencias del personal de TI lo que provoca brechas en las habilidades que poseen estos respecto a las nuevas tecnologías o métodos. (INTERNO)
	51	No se encuentran claramente definidas las habilidades y competencias necesarias para ocupar un puesto en TI.
Determinar si la entidad tiene definida las políticas relativas a TI y promueve la cooperación interdepartamental así como cumplimiento de dichas políticas.	*50*	Errores en el manejo de procesos e información debido a un personal desinformado o poco preparado.
	54	Falta de conocimiento y entendimiento del negocio incluidas las políticas relacionadas a TI afectando la calidad de los servicios entregados.
Determinar si existe un proceso para tratar el riesgo de programas o proyectos de áreas o eventos que pueden causar consecuencias negativas así como su punto de registro. *Determinar la existencia de una guía referencial que cubra el ciclo de vida de los proyectos, en la que se defina criterios referenciales, gestión de riesgos y se resalte la necesidad de aportar o aumentar la capacidad del negocio*	*13*	Descuido de la documentación relacionada con los proyectos considerados en el portafolio.
	18	Ausencia de un proceso para el análisis de riesgo de un proyecto o inefectividad del mismo.
	19	Criterios claves de rendimiento del proyecto no definidos claramente.
	15	Planificación inadecuada de los proyectos
	24	Falta de claridad en los pasos claves para cerrar un proyecto.
	25	Desviaciones del rendimiento de los proyectos frente a los requerimientos iniciales y ausencia de un análisis posterior.
	11	Enfoque desactualizado de la gestión de programas y proyectos.
	31	Actividades incompletas sin identificar y comunicar.
Verificar que todos los requerimientos y soluciones han sido previamente aprobadas antes de su desarrollo, implementación o adquisición	*84*	Existencia de dudas por parte del usuario sobre la arquitectura de procesos e información.
	17	Ausencia o ineficiencia de un plan de gestión de calidad para los entregables del proyecto

Verificar que los procedimientos y tareas dentro de TI son desarrolladas de manera confiable y consistente, así como el manejo de respaldos según un determinado procedimiento	*119*	Inobservancia de los requerimientos de control de la información en los procesos de negocio, lo cual imposibilita hacer frente a los riesgos de la información y el cumplimiento de regulaciones y leyes.
	121	No se ejecutan procedimientos y mecanismos que permitan mejorar el nivel de satisfacción de los usuarios.
	122	No hay un enfoque hacia la gestión del cumplimiento tanto para objetivos como para su rendimiento.
	118	Falta de establecimiento de medidas para supervisar y recolectar datos del nivel del servicio lo que imposibilita la obtención de información de las mejoras.
	112	No se realiza ni se da a conocer a las partes los resultados de las revisiones post-implementación.
	5	Falta de seguimiento y control de las soluciones implementadas.
Determinar si la organización mantiene relaciones con las partes interesadas que le permitan trabajar en conjunto y faciliten la identificación del uso de nuevas tecnologías	*7*	Las partes interesadas no son participantes activas para la entidad.
	10	Falta de involucramiento de las partes interesadas en el ciclo de proyectos, lo que genera un incremento de costes por uso adicional de recursos si existen brechas en las especificaciones o servicios al usuario final.
	32	Descoordinación en las inversiones importantes relacionadas con TI debido a la falta de comunicación con los altos mandos de la institución, lo que imposibilita el cumplimiento de los objetivos estratégicos planteados.
	21	Desconocimiento de las condiciones de aceptación de terceras partes.
	164	Falta de periodicidad en las reuniones para informar sobre la posibilidad de adopción de nuevas tecnologías y los beneficios de estas para la entidad.
Determinar la participación conjunta de la organización y las partes interesadas para la coordinación de todo lo relacionado a entrega de servicios así como soluciones por parte de TI a problemas del negocio	*36*	Intercambio de información inoportuna e insuficiente con las partes interesadas.
	8	Requerimientos no comunicados ni aprobados antes de su puesta en marcha.
	16	Deficiencias en la comunicación verbal o escrita adoptada durante el desarrollo del ciclo de vida de un proyecto.
	99	Los cambios aprobados no son comunicados oportunamente a los actores y usuarios relacionados
	92	Fallas en la divulgación o concientización de las políticas relacionadas a TI.

	163	Escasez de mecanismos para promover y captar ideas de los empleados.
Determinar que las instalaciones de TIC están adecuadamente gestionadas respecto de riesgos, electricidad, telecomunicaciones y demás	*150*	Mala configuración de equipamientos de seguridad.
	79	Desconocimiento de políticas de seguridad en la conectividad
	56	Falta de concientización y participación del personal en acciones preventivas que se direccionen a evitar los riesgos de salud y seguridad en el trabajo.
Establecer que la organización ha definido una política de continuidad basada en los objetivos del negocio y los intereses de las partes interesadas	*27*	Degradación de la imagen de la entidad por su incapacidad para responder oportuna y asertivamente contra incidentes que afectan a los servicios entregados por proyectos ineficientes.
	68	Falta de un plan de continuidad que imposibilita responder a incidentes e interrupciones de servicios.
	146	Exposición alta a daños por ejecución de malware.
Determinar si existe un proceso de protección contra software malicioso (malware) que permita proteger a la información de manera íntegra	*86*	Ausencia de alineación de las prácticas manejadas en el área de TI con estándares internacionales y códigos de gobierno.
	139	Políticas de prevención y tratamiento de software malicioso desactualizadas o ausencia de las mismas.
	140	Desactualización de los usuarios respecto a configuraciones de tráfico entrante, uso de correos electrónicos y descargas lo cual facilita el acceso de software malicioso (virus, gusanos, software espía y correo basura).
	141	Registro de incidentes de seguridad desactualizado lo que imposibilita su evaluación, investigación y retroalimentación.
	144	Desconocimiento de los incidentes provocados por malware con datos específicos de cada uno de ellos.
	154	Ataques de virus, gusanos, troyanos, rootkits, spyware, etc.
Corroborar que la gestión de seguridad de los puestos de usuario final está siendo llevada a cabo óptimamente mediante procedimientos que permitan deshacerse de dispositivos de usuario final de manera segura	*93*	Fallas en los registros y definición de acceso a los activos físicos de TI o el uso de dispositivos por parte del usuario para tratamiento de la información.
	134	Ineficiencia o ausencia de dispositivos que detectan las amenazas del entorno, debido a la falta de supervisión, mantenimiento y actualización de los mismos.

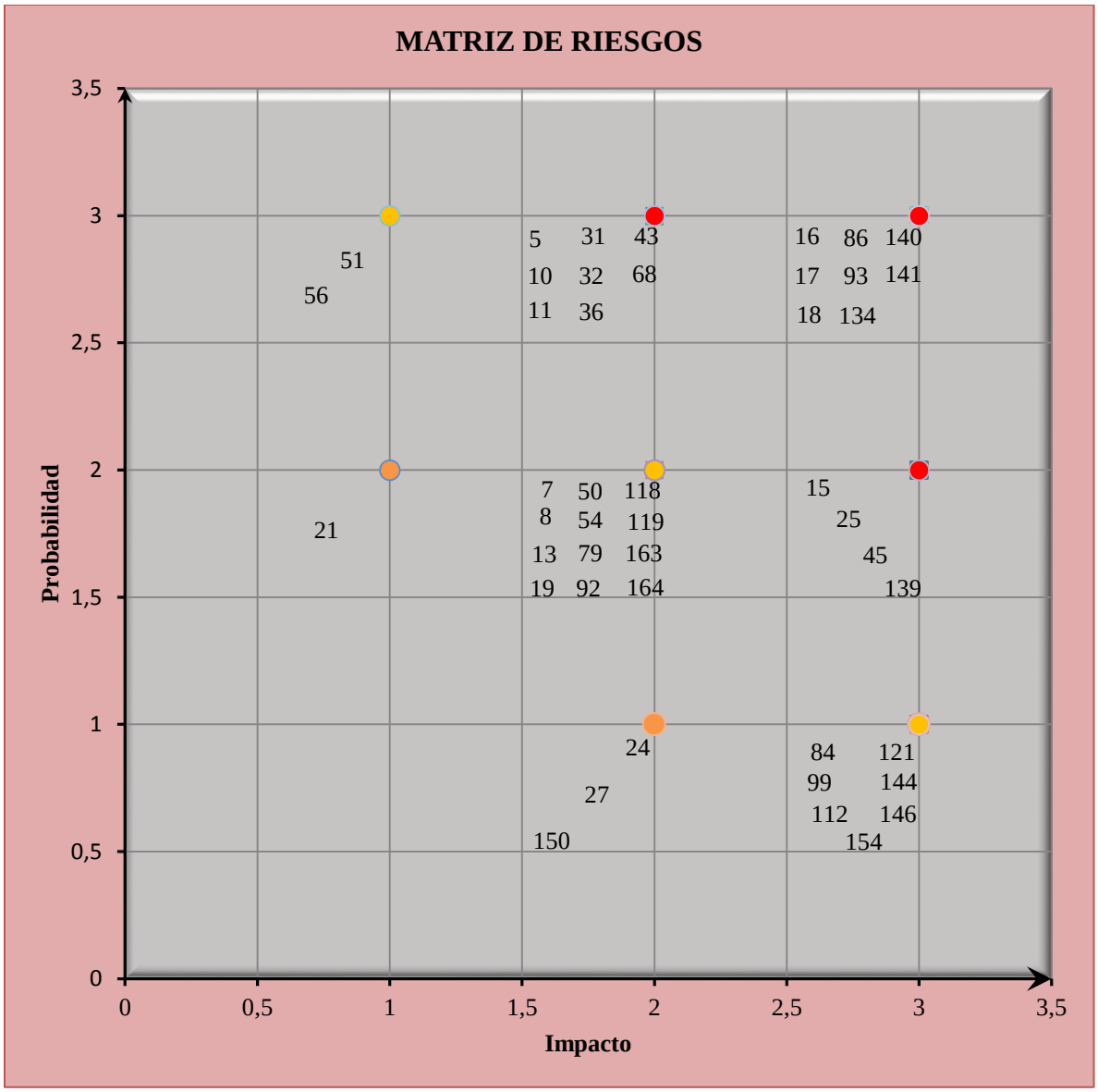
Fuente: Autoras

Anexo 9: Evaluación del Riesgo

N° de Riesgo	RIESGO	EVALUACIÓN AL RIESGO			
		NIVEL DE RIESGO			
		Probabilidad	Impacto	Cuantitativo	Cualitativo
43	Inexistencia de métodos para la evaluación del personal.	3	2	6	NT
45	Ausencia de planes de desarrollo-mejora de habilidades y competencias del personal de TI lo que provoca brechas en las habilidades que poseen estos respecto a las nuevas tecnologías o métodos. (INTERNO)	2	3	6	NT
51	No se encuentran claramente definidas las habilidades y competencias necesarias para ocupar un puesto en TI.	3	1	3	A
50	Errores en el manejo de procesos e información debido a un personal desinformado o poco preparado.	2	2	4	A
54	Falta de conocimiento y entendimiento del negocio incluidas las políticas relacionadas a TI afectando la calidad de los servicios entregados.	2	2	4	A
13	Descuido de la documentación relacionada con los proyectos considerados en el portafolio.	2	2	4	A
18	Ausencia de un proceso para el análisis de riesgo de un proyecto o inefectividad del mismo.	3	3	9	NT
19	Criterios claves de rendimiento del proyecto no definidos claramente.	2	2	4	A
15	Planificación inadecuada de los proyectos	2	3	6	NT
24	Falta de claridad en los pasos claves para cerrar un proyecto.	1	2	2	M
25	Desviaciones del rendimiento de los proyectos frente a los requerimientos iniciales y ausencia de un análisis posterior.	2	3	6	NT
11	Enfoque desactualizado de la gestión de programas y proyectos.	3	2	6	NT
31	Actividades incompletas sin identificar y comunicar.	3	2	6	NT
84	Existencia de dudas por parte del usuario sobre la arquitectura de procesos e información.	1	3	3	A
17	Ausencia o ineficiencia de un plan de gestión de calidad para los entregables del proyecto	3	3	9	NT
119	Inobservancia de los requerimientos de control de la información en los procesos de negocio, lo cual imposibilita hacer frente a los riesgos de la información y el cumplimiento de regulaciones y leyes.	2	2	4	A
121	No se ejecutan procedimientos y mecanismos que permitan mejorar el nivel de satisfacción de los usuarios.	1	3	3	A
122	No hay un enfoque hacia la gestión del cumplimiento tanto para objetivos como para su rendimiento.	3	2	6	NT
118	Falta de establecimiento de medidas para supervisar y recolectar datos del nivel del servicio lo que imposibilita la obtención de información de las mejoras.	2	2	4	A
112	No se realiza ni se da a conocer a las partes los resultados de las revisiones post-implementación.	1	3	3	A
5	Falta de seguimiento y control de las soluciones implementadas.	3	2	6	NT
7	Las partes interesadas no son participantes activas para la entidad.	2	2	4	A
10	Falta de involucramiento de las partes interesadas en el ciclo de proyectos, lo que genera un incremento de costes por uso adicional de recursos si existen brechas en las especificaciones o servicios al usuario final.	3	2	6	NT
32	Descoordinación en las inversiones importantes relacionadas con TI debido a la falta de comunicación con los altos mandos de la institución, lo que imposibilita el cumplimiento de los objetivos estratégicos planteados.	3	2	6	NT
21	Desconocimiento de las condiciones de aceptación de terceras partes.	2	1	2	M
164	Falta de periodicidad en las reuniones para informar sobre la posibilidad de adopción de nuevas tecnologías y los beneficios de estas para la entidad.	2	2	4	A
36	Intercambio de información inoportuna e insuficiente con las partes interesadas.	3	2	6	NT
8	Requerimientos no comunicados ni aprobados antes de su puesta en marcha.	2	2	4	A
16	Deficiencias en la comunicación verbal o escrita adoptada durante el desarrollo del ciclo de vida de un proyecto.	3	3	9	NT
99	Los cambios aprobados no son comunicados oportunamente a los actores y usuarios relacionados	1	3	3	A
92	Fallas en la divulgación o concientización de las políticas relacionadas a TI.	2	2	4	A
163	Escasez de mecanismos para promover y captar ideas de los empleados.	2	2	4	A
150	Mala configuración de equipamientos de seguridad.	1	2	2	M
79	Desconocimiento de políticas de seguridad en la conectividad	2	2	4	A
56	Falta de concientización y participación del personal en acciones preventivas que se direccionen a evitar los riesgos de salud y seguridad en el trabajo.	3	1	3	A
27	Degradación de la imagen de la entidad por su incapacidad para responder oportuna y asertivamente contra incidentes que afectan a los servicios entregados por proyectos ineficientes.	1	2	2	B
68	Falta de un plan de continuidad que imposibilita responder a incidentes e interrupciones de servicios.	3	2	6	NT
146	Exposición alta a daños por ejecución de malware.	3	1	3	M
86	Ausencia de alineación de las prácticas manejadas en el área de TI con estándares internacionales y códigos de gobierno.	3	3	9	NT
139	Políticas de prevención y tratamiento de software malicioso desactualizadas o ausencia de las mismas.	2	3	6	NT
140	Desactualización de los usuarios respecto a configuraciones de tráfico entrante, uso de correos electrónicos y descargas lo cual facilita el acceso de software malicioso (virus, gusanos, software espía y correo basura).	3	3	9	NT
141	Registro de incidentes de seguridad desactualizado lo que imposibilita su evaluación, investigación y retroalimentación.	3	3	9	NT
144	Desconocimiento de los incidentes provocados por malware con datos específicos de cada uno de ellos.	1	3	3	A
154	Ataques de virus, gusanos, troyanos, rootkits, spyware, etc.	1	3	3	A
93	Fallas en los registros y definición de acceso a los activos físicos de TI o el uso de dispositivos por parte del usuario para tratamiento de la información.	3	3	9	NT
134	Ineficiencia o ausencia de dispositivos que detectan las amenazas del entorno, debido a la falta de supervisión, mantenimiento y actualización de los mismos.	3	3	9	NT

Fuente: Autoras

Anexo 10: Matriz de Riesgos



Fuente: Autoras

NIVEL DE RIESGO		
COLOR	CALF.	EXPRESIÒN
	6 o 9	Intolerable
	3 o 4	Tolerable
	2	Moderado
	1	Aceptable

Anexo 11: Plan de Comunicación del Riesgo

PLAN DE COMUNICACIÓN DEL RIESGO

CICLO DE VIDA Y PARTES INTERESADAS	ETAPAS	FRECUENCIA	PARTES RELACIONAS		MEDIOS		
			INTERNAS	EXTERNAS	ESCRITO	VERBAL	VIRTUAL
	Planear						
	Diseñar						
	Adquirir						
	Uso						
	Monitoreo						
	Disposición						

METAS	SUBDIMENSIONES CUALITATIVAS Y METAS		INTERNAS	EXTERNAS
	INTRÍNSECA	Precisión		
		Objetividad		
		Credibilidad		
		Reputación		
	CONTEXTUAL Y DE REPRESENTACIÓN	Relevancia		
		Integridad		
		Oportunidad		
		Suficiencia		
		Concisa		
		Consistente		
		Interpretable		
		Entendible		
		Manipulación		
	SEGURIDAD	Disponibilidad		
		Acceso Restringido		

Fecha:_____

Responsable:_____

Fuente: (ISACA, 2013)
Adaptado: Autoras

Anexo 12: Modelo de Informe

Cuenca, XX de XXX XXX

Director de Tecnologías de Información y Comunicación
Ing. Patricio Guerrero
Cuidad

De mis consideraciones:

Mediante la presente se pone a su conocimiento el resultado del análisis de riesgo de las Tecnologías de Información y Comunicación efectuado por las señoritas Daisy Alvarado Carpio y Alexandra Zumba Morales al área en la cual usted se desempeña.

Cabe recalcar que dicho análisis se ha desarrollado con base y apoyo a la metodología que presenta COBIT 5 *para* riesgos permitiendo este marco vincularlo y al mismo tiempo identificar riesgos por el incumplimiento de la normativa de control interno emanada por la Contraloría General del Estado de nuestro país. Los riesgos potenciales levantados se encuentran adjunto a la presente junto con la matriz de riesgos para su evaluación oportuna y por consiguiente un inmediata respuesta para tratarlos.

De antemano agradecemos su atención.

Atentamente,

Daisy Alvarado C.	Alexandra Zumba M.
0104368600	0105445803

Adj: Listado de Riesgos y Matriz de Riesgos

Fuente: Autoras

N° de Riesgo	RIESGO	CATEGORÍAS																		ACTOR		TIPO DE AMENAZA			EVENTO								VALORACIÓN		DETECCIÓN		
		Establecimiento y mantenimiento del portafolio	Gestión del ciclo de vida del programa o proyecto	Decisión de hacer Inversión TI	Experiencia y habilidades en TI	Información (Violación de datos: daños, fuga y acceso)	Arquitectura	Infraestructura	Software	Propiedad de un negocio de	Proveedores	Cumplimiento regulatorio	Robo o destrucción de	Malware	Ataques lógicos	Acción industrial	Ambiente	Hechos de la naturaleza	Innovación	Interno	Externo	Malicioso	Error	Falla	Revelación	Interrupción	Modificación	Robo	Destrucción	Diseño Inefectivo	Leyes y Regulación	Uso Inapropiado	Recurso	Activo	Lenta	Moderada	Instantánea
43	Inexistencia de métodos para la evaluación del personal.				■															■				■						■			■			■
45	Ausencia de planes de desarrollo-mejora de habilidades y competencias del personal de TI lo que provoca brechas en las habilidades que poseen estos respecto a las nuevas tecnologías o métodos. (INTERNO)				■															▒				▒						▒			▒		▒		
51	No se encuentran claramente definidas las habilidades y competencias necesarias para ocupar un puesto en TI.				■															■			■							■			■		■		
50	Errores en el manejo de procesos e información debido a un personal desinformado o poco preparado.				■															▒			▒						▒				▒			▒	
54	Falta de conocimiento y entendimiento del negocio incluidas las políticas relacionadas a TI afectando la calidad de los servicios entregados.				■															■				■						■			■				■
13	Descuido de la documentación relacionada con los proyectos considerados en el portafolio.		■																	■	■			■			■						■			■	
18	Ausencia de un proceso para el análisis de riesgo de un proyecto o inefectividad del mismo.		■																	▒			▒	▒						▒			▒	▒			▒
19	Criterios claves de rendimiento del proyecto no definidos claramente.		■																	■				■						■			■				■
15	Planificación inadecuada de los proyectos		■																	▒				▒					▒				▒	▒		▒	
24	Falta de claridad en los pasos claves para cerrar un proyecto.		■																	■	■		■			■							■			■	
25	Desviaciones del rendimiento de los proyectos frente a los requerimientos iniciales y ausencia de un análisis posterior.		■																	▒			▒				▒						▒		▒		
11	Enfoque desactualizado de la gestión de programas y proyectos.		■																	■				■						■				■			■
31	Actividades incompletas sin identificar y comunicar.		■																	▒			▒		▒								▒			▒	
84	Existencia de dudas por parte del usuario sobre la arquitectura de procesos e información.						■													■	■		■		■								■			■	
17	Ausencia o ineficiencia de un plan de gestión de calidad para los entregables del proyecto		■																	▒			▒	▒	▒								▒			▒	▒
119	Inobservancia de los requerimientos de control de la información en los procesos de negocio, lo cual imposibilita hacer frente a los riesgos de la información y el cumplimiento de regulaciones y leyes.								■											■				■				■				■			■	
121	No se ejecutan procedimientos y mecanismos que permitan mejorar el nivel de satisfacción de los usuarios.								■											▒				▒					▒				▒				▒
122	No hay un enfoque hacia la gestión del cumplimiento tanto para objetivos como para su rendimiento.								■											■				■					■				■				■
118	Falta de establecimiento de medidas para supervisar y recolectar datos del nivel del servicio lo que imposibilita la obtención de información de las mejoras.								■											■			■							■			■			■	

112	No se realiza ni se da a conocer a las partes los resultados de las revisiones post-implementación.	
5	Falta de seguimiento y control de las soluciones implementadas.	
7	Las partes interesadas no son participantes activas para la entidad.	
10	Falta de involucramiento de las partes interesadas en el ciclo de proyectos, lo que genera un incremento de costes por uso adicional de recursos si existen brechas en las especificaciones o servicios al usuario final.	
32	Descoordinación en las inversiones importantes relacionadas con TI debido a la falta de comunicación con los altos mandos de la institución, lo que imposibilita el cumplimiento de los objetivos estratégicos planteados.	
21	Desconocimiento de las condiciones de aceptación de terceras partes.	
164	Falta de periodicidad en las reuniones para informar sobre la posibilidad de adopción de nuevas tecnologías y los beneficios de estas para la entidad.	
36	Intercambio de información inoportuna e insuficiente con las partes interesadas.	
8	Requerimientos no comunicados ni aprobados antes de su puesta en marcha.	
16	Deficiencias en la comunicación verbal o escrita adoptada durante el desarrollo del ciclo de vida de un proyecto.	
99	Los cambios aprobados no son comunicados oportunamente a los actores y usuarios relacionados	
92	Fallas en la divulgación o concientización de las políticas relacionadas a TI.	
163	Escasez de mecanismos para promover y captar ideas de los empleados.	
150	Mala configuración de equipamientos de seguridad.	
79	Desconocimiento de políticas de seguridad en la conectividad	
56	Falta de concientización y participación del personal en acciones preventivas que se direccionen a evitar los riesgos de salud y seguridad en el trabajo.	
27	Degradación de la imagen de la entidad por su incapacidad para responder oportuna y asertivamente contra incidentes que afectan a los servicios entregados por proyectos ineficientes.	
68	Falta de un plan de continuidad que imposibilita responder a incidentes e interrupciones de servicios.	
146	Exposición alta a daños por ejecución de malware.	
86	Ausencia de alineación de las prácticas manejadas en el área de TI con estándares internacionales y códigos de gobierno.	
139	Políticas de prevención y tratamiento de software malicioso desactualizadas o ausencia de las mismas.	
140	Desactualización de los usuarios respecto a configuraciones de tráfico entrante, uso de correos electrónicos y descargas lo cual facilita el acceso de software malicioso (virus, gusanos, software espía y correo basura).	
141	Registro de incidentes de seguridad desactualizado lo que imposibilita su evaluación, investigación y retroalimentación.	
144	Desconocimiento de los incidentes provocados por malware con datos específicos de cada uno de ellos.	
154	Ataques de virus, gusanos, troyanos, rootkits, spyware, etc.	
93	Fallas en los registros y definición de acceso a los activos físicos de TI o el uso de dispositivos por parte del usuario para tratamiento de la información.	
134	Ineficiencia o ausencia de dispositivos que detectan las amenazas del entorno, debido a la falta de supervisión, mantenimiento y actualización de los mismos.	

Fuente: Autoras

Anexo 13: Acciones para tratar el Riesgo

N°	RIESGO	NIVEL DE RIESGO		ACTIVIDADES							
				DESCRIPCIÓN	RECURSOS				RESPONSABLES		MÉTRICAS RELACIONADAS
		CUANTITATIVO	CUALITATIVO		Información	Aplicaciones	Infraestructur	Personas	RESPONSABLE* ¿Quién hace?	RINDE CUENTAS* ¿Quién comunica?	
86	Ausencia de alineación de las prácticas manejadas en el área de TI con estándares internacionales y códigos de gobierno.	9	NT	Diseñar y plantear políticas para garantizar el control de TI en temas claves considerando su alineación con estándares y códigos de gobierno y gestión. Ajustar las políticas implementadas como mínimo una vez al año.	X			X	INSTITUCIÓN: Director Administrativo DTIC: Director de TIC, Ingeniero 2 Infraestructura de TI	Rectorado	Porcentaje de políticas soportadas por estándares y prácticas internacionales efectivas. Frecuencia de revisión y actualización de las políticas. Porcentaje de políticas y estándares documentadas y actualizadas.
45	Ausencia de planes de desarrollo-mejora de habilidades y competencias del personal de TI lo que provoca brechas en las habilidades que poseen estos respecto a las nuevas tecnologías o métodos. (INTERNO)	6	NT	Identificar las competencias y habilidades requeridas así como existentes, que apoyan la consecución de objetivos para luego plantear los planes de desarrollo y formación del personal basado en dichos resultados; de esta manera esta serán conforme la realidad de las necesidades.	X			X	INSTITUCIÓN: Coordinador/a Administrativo de la Unidad de Planificación física y ejecución de obras, Director de Talento Humano DTIC: Coordinador de Sistemas de Información, Ingeniero 3 Unidad de Centro de Desarrollo de Software, Ingeniero 3 Unidad de Operaciones de Sistemas Informáticos, Ingeniero 2 Infraestructura de TI, Ingeniero 3 de Servicios de CSE, Ingeniero 3 de Seguridad CRC	Director de TIC	Número de empleados de la D TIC evaluados/Total de empleados de la DTIC. Número de propuestas ejecutadas/Número de propuestas ejecutadas. Número de horas de formación reales/Número de horas planeadas de formación
43	Inexistencia de métodos para la evaluación del personal.	6	NT	Aplicación de una evaluación de desempeño 360° y desarrollar planes de mejora basados en los resultados de la evaluación así como de las brechas identificadas del personal.				X	INSTITUCIÓN: Director de Planificación, Director de Talento Humano DTIC: Ingeniero 3 Unidad de Centro de Desarrollo de Software, Ingeniero 3 Unidad de Operaciones de Sistemas Informáticos, Ingeniero 3 de Servicios, Ingeniero 3 de Seguridad.	Coordinador de Sistemas de Información	Porcentaje de puestos vacantes. Frecuencia de las evaluaciones del personal entrante como antiguo.
11	Enfoque desactualizado de la gestión de programas y proyectos.	6	NT	Actualizar el enfoque de gestión de proyectos o programas conforme cambian las necesidades de la entidad así como las mejores prácticas existentes. Asegurar que el enfoque cubra en su totalidad el ciclo de vida de un proyecto utilizando ya sea PMBOK o PMI en lugar de RUP.	X				INSTITUCIÓN: Coordinador/a de la Unidad de Relaciones Públicas y Comunicación, Coordinador/a de la Unidad de Planificación Estratégica DTIC: Director de TIC	Rectorado	Número de veces que se ha actualizado el enfoque de gestión de programas o proyectos.
36	Intercambio de información inoportuna e insuficiente con las partes interesadas.	6	NT	Identificar y comprometer a las partes interesadas asegurándose de poseer una base de datos actualizados con el fin de gestionar reuniones periódicas y enviar informes ya sean físicos o virtuales fomentando de esta manera el intercambio de información precisa, consistente y oportuna durante todo el ciclo de vida de un proyecto. Gestionar la creación de foros de consulta para solucionar dudas o inconvenientes en temas de ocurrencia cotidiana evitando la generación de trámites extensos para su respuesta.				X	INSTITUCIÓN: Director Administrativo, Coordinador/a de la Unidad de Relaciones Públicas y Comunicación, Coordinador/a Administrativo de la Unidad de Planificación física y ejecución de obras DTIC: Director de TIC	Rectorado	Nivel de satisfacción de las partes interesadas con el alcance del portafolio de programas y servicios planeados. Porcentaje de inversiones de TI en los que la realización del beneficio se monitoriza través del ciclo de vida económico completo Porcentaje de partes interesadas efectivamente comprometidas.
15	Planificación inadecuada de los proyectos.	6	NT	Definir aspectos claves dentro de los planes que se relacionen con costos, personas, actividades, tiempo, responsabilidades e indicadores con la coordinación y participación de las distintas unidades afectadas por el proyecto teniendo en cuenta su desagregación por cada una de las fases.	X			X	INSTITUCIÓN: Coordinador/a de la Unidad de Control DTIC: Director de TIC, Coordinador de Sistemas Informáticos, Coordinador de Redes y Comunicaciones, Coordinador de Sistemas de Información.	Coordinador/a Administrativo de la Unidad de Planificación física y ejecución de obras	Número de desviaciones presentadas/ Total de proyectos realizados. Número de Proyectos realizados y comunicados/Total de proyectos realizados. Número de informes de progreso/Total de proyectos realizados.

16	Deficiencias en la comunicación verbal o escrita adoptada durante el desarrollo del ciclo de vida de un proyecto.	9	NT	Asegurar la comunicación efectiva de los planes aprobados, el progreso y los cambios generados, mediante el uso de informes para facilitar a la dirección el control y conocimiento de lo ejecutado. Diseñar, implementar y mantener un plan de comunicación que sirva de apoyo para llevar a cabo los procesos y actividades generales de la entidad.	X	X		X	INSTITUCIÓN: Coordinador/a de la Unidad de Control DTIC: Director de TIC	Coordinador/a Administrativo de la Unidad de Planificación física y ejecución de obras	Número de programas/proyectos ejecutados en plazo. Porcentaje de proyectos emprendidos sin casos de negocio aprobados.
17	Ausencia o ineficiencia de un plan de gestión de calidad para los entregables del proyecto	9	NT	Adopción de la ISO 9001 para temas relacionados con proyectos mientras que ITIL se destinará para la mejora de la calidad en cuanto a la prestación de servicios de TI, los cuales permiten el logro de sus objetivos. Además es necesario definir parámetros de calidad mínimos para los proyectos.	X		X		INSTITUCIÓN: Coordinador/a de la Unidad de Relaciones Públicas y Comunicación, Coordinador/a de la Unidad de Control DTIC: Ingeniero 3 Unidad de Centro de Desarrollo de Software	Coordinador/a Administrativo de la Unidad de Planificación física y ejecución de obras	Porcentaje de revisiones de calidad anuales
18	Ausencia de un proceso para el análisis de riesgo de un proyecto o inefectividad del mismo.	9	NT	Definir un enfoque para gestionar los riesgos como ISO 27005, 31000, COBIT 5 o COSO ERM y asignar responsabilidades, para después proceder a la aplicación de un análisis de riesgos que cuantifique los mismos.	X			X	INSTITUCIÓN: Coordinador/a de la Unidad de Relaciones Públicas y Comunicación, Coordinador/a de la Unidad de Control DTIC: Director de TIC, Coordinador de Sistemas Informáticos, Coordinador de Redes y Comunicaciones, Coordinador de Sistemas de Información.	Coordinador/a Administrativo de la Unidad de Planificación física y ejecución de obras	Número de proyectos analizados/Total de proyectos. Número de incidentes identificados. Número de proyectos analizados con incidentes/Total de proyectos analizados.
25	Desviaciones del rendimiento de los proyectos frente a los requerimientos iniciales y ausencia de un análisis posterior.	6	NT	Comparar el rendimiento real del proyecto versus los criterios iniciales e identificar causas. Supervisar los cambios aprobados y generar informes.	X	X			INSTITUCIÓN: Coordinador/a de la Unidad de Control, Auditor/a General DTIC: Ingeniero 3 Unidad de Centro de Desarrollo de Software	Coordinador/a Administrativo de la Unidad de Planificación física y ejecución de obras	Número de requisitos cumplidos/ Número de requisitos planteados. Número Eventos investigados/Total de eventos.
31	Actividades incompletas sin identificar y comunicar.	6	NT	Definir pasos claves para cerrar un proyecto. Identificar y rastrear aquellas actividades incompletas mediante un seguimiento del cumplimiento de lo planteado en el cronograma de actividades de manera que permita cumplir con el propósito del proyecto para que sean remediadas oportunamente.	X	X		X	INSTITUCIÓN: Coordinador/a de la Unidad de Control	Coordinador/a Administrativo de la Unidad de Planificación física y ejecución de obras	Número de actividades incompletas/Total de actividades del proyecto. Porcentaje de comunicaciones sobre actividades incompletas
10	Falta de involucramiento de los usuarios en el ciclo de proyectos, lo que genera un incremento de costes por uso adicional de recursos si existen brechas en las especificaciones o servicios al usuario final.	6	NT	Identificar, obtener, analizar y confirmar los requerimientos de todas las partes interesadas durante todo el proyecto para proceder a la priorización de aquellos requerimientos técnicos y funcionales de forma que se pueda contrarrestar a los riesgos de información y cumplimiento con regulaciones y leyes.	X	X		X	INSTITUCIÓN: Coordinador/a de la Unidad de Control DTIC: Coordinador de Sistemas de Información, Ingeniero 3 Unidad de Centro de Desarrollo de Software	Coordinador/a Administrativo de la Unidad de Planificación física y ejecución de obras	Porcentaje de requerimientos repetidos debido a la no alineación entre las necesidades y expectativas de la organización. Número de partes interesadas satisfechas/Total de Requerimientos.
5	Falta de seguimiento y control de las soluciones implementadas.	6	NT	Desarrollar un plan de mantenimiento de las soluciones para detectar y tratar cambios en las necesidades de usuarios y posteriormente confirmar la aceptación de aspectos claves; se debe resaltar las responsabilidades y la periodicidad de la aplicación de dicho plan así como los métodos de evaluación a emplear.	X			X	INSTITUCIÓN; Coordinador/a de la Unidad de Control DTIC: Director de TIC, Ingeniero 3 de Servicios de CSE	Ingeniero 3 Unidad de Centro de Desarrollo de Software	Número de soluciones revisadas/Total de proyectos
32	Descoordinación en las inversiones importantes relacionadas con TI debido a la falta de comunicación con la alta dirección de la institución, lo que imposibilita el cumplimiento de los objetivos estratégicos planteados.	6	NT	Determinar un grupo de trabajo efectivo cuyos miembros incluirán delegados de la alta dirección, personal de TI, terceros externos y agentes de cambios quienes con sus actividades comunes y metas conjuntas logarán una comunicación óptima en pro para el cumplimiento de los objetivos institucionales.				X	INSTITUCIÓN: Coordinador/a Administrativo de la Unidad de Planificación física y ejecución de obras, Coordinador/a de la Unidad de Control DTIC: Director de TIC, Ingeniero 3 Unidad de Centro de Desarrollo de Software	Coordinador/a de la Unidad de Relaciones Públicas y Comunicación	Número de programas/proyectos ejecutados en plazo y en presupuesto. Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto. Nivel de concienciación y comprensión de las posibilidades de innovación de TI con relación a la institución.

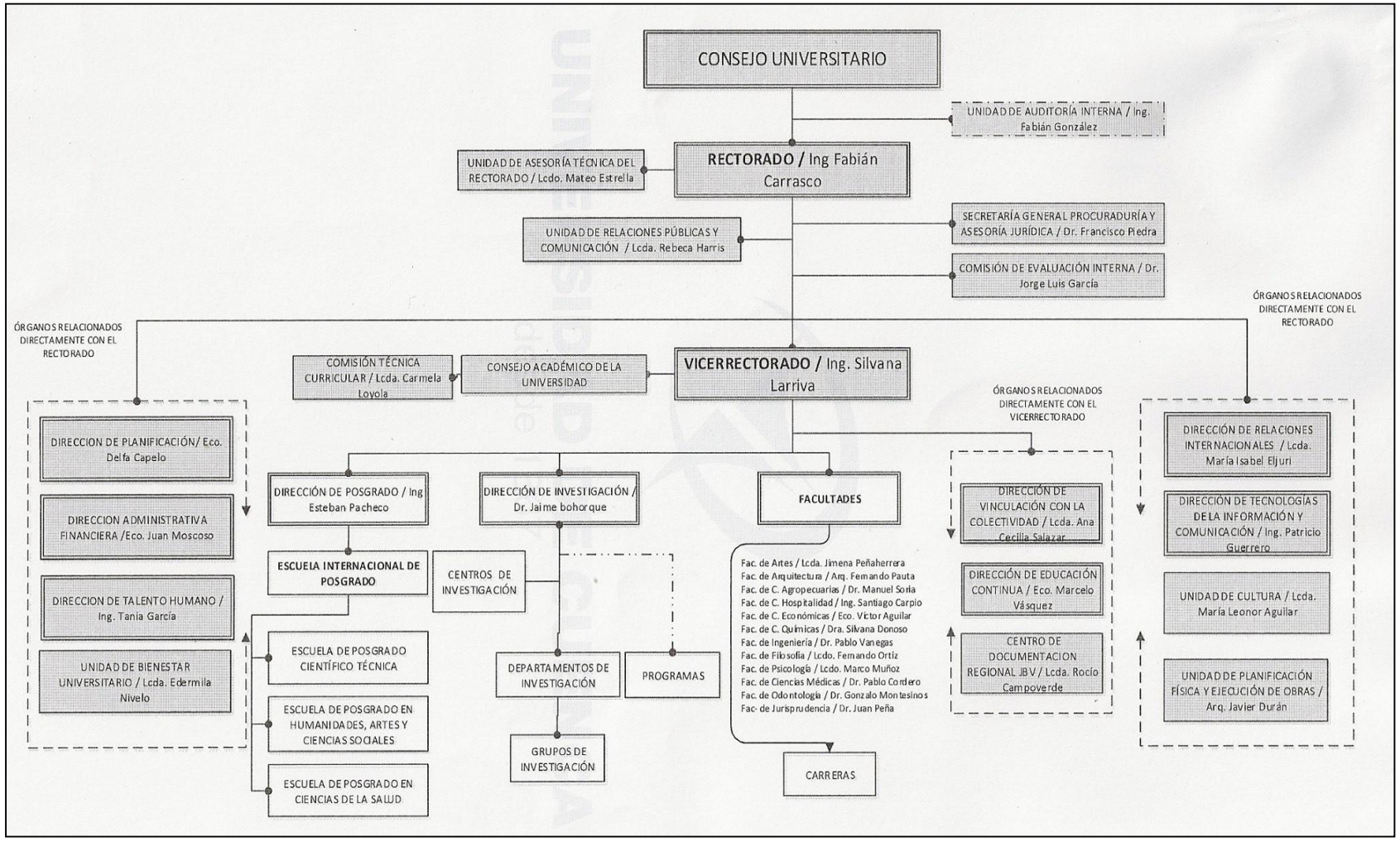
Daisy Fernanda Alvarado Carpio
Laura Alexandra Zumba Morales

68	Falta de un plan de continuidad que imposibilita responder a incidentes e interrupciones de servicios.	6	NT	Desarrollar políticas de continuidad de negocio. Diseñar e implementar un Plan de Continuidad de Negocio que partirá de un análisis de riesgo de los procesos críticos del negocio lo cual permitirá definir las estrategias que se adoptarán para evitar la interrupción de operaciones definiendo, responsables, recursos, acciones, pruebas, mantenimiento y revisión de dicho plan. Además incluir en el plan de comunicación los aspectos específicos para casos emergentes.	X	X	X	X	INSTITUCIÓN: Coordinador/a de la Unidad de Planificación Estratégica, Unidad de Auditoría Interna DTIC: Director de TIC, Coordinador de Sistemas de Información, Ingeniero 2 Infraestructura de TI	Coordinador/a de la Unidad de Control	Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos. Número de interrupciones del negocio debidas a incidentes en el servicio de TI. Porcentaje de mejoras acordadas que han sido reflejadas en el plan. Porcentaje de asuntos identificados que se han incluido satisfactoriamente en el plan.
134	Ineficiencia o ausencia de dispositivos que detectan las amenazas del entorno, debido a la falta de supervisión, mantenimiento y actualización de los mismos.	9	NT	Instalar equipamiento de TI, móvil y fuera de las instalaciones que permitan la identificación de eventualidades naturales así como aquellas provocadas por el ser humano monitorizando periódicamente su funcionamiento. Revisar que las políticas implementadas impidan o limiten acciones que puedan ocasionar incendios u otros. (comer, fumar, beber, almacenamiento de suministros y materiales de oficinas en áreas sensibles)			X		INSTITUCIÓN: Dirección Financiera DTIC: Ingeniero 3 Unidad de Operaciones de Sistemas Informáticos, Ingeniero 3 de Seguridad CRC, Ingeniero 2 Infraestructura de TI	Director de TIC	Porcentaje de tipos de eventos operativos críticos cubiertos por los sistemas de detección automática.
139	Políticas de prevención y tratamiento de software malicioso desactualizadas o ausencia de las mismas.	6	NT	Definir políticas relacionadas con los permisos para descargar e instalar programas o software por parte de un usuario en su unidad de trabajo que sean complementarios a los ya establecidos. Establecer procedimientos que sirvan de herramientas para el logro de dicha política, enfocadas en la supervisión dejando opción a que se faltaré a dicha política en casos emergentes siempre que estos estén debidamente fundamentados y aprobados.	X	X			INSTITUCIÓN: Director de Talento Humano. DTIC: Ingeniero 3 Unidad de Centro de Desarrollo de Software, Ingeniero 3 Unidad de Operaciones de Sistemas Informáticos, Ingeniero 3 de Seguridad CRC	Director de TIC	Número de descargas de programas tratados / Total de descargas efectuadas.
140	Desactualización de los usuarios respecto a configuraciones de tráfico entrante, uso de correos electrónicos y descargas lo cual facilita el acceso de software malicioso (virus, gusanos, software espía y correo basura).	9	NT	Capacitar a los diferentes usuarios sobre procedimientos y responsabilidades de prevención lo cual permita la sensibilización y el entendimiento de la importancia de la seguridad y protección de la información.	X			X	INSTITUCIÓN: Director de Talento Humano. DTIC: Ingeniero 3 Unidad de Centro de Desarrollo de Software, Ingeniero 3 Unidad de Operaciones de Sistemas Informáticos, Ingeniero 3 de Seguridad CRC	Director de TIC	Número de vulnerabilidades. Porcentaje de pruebas periódicas de los dispositivos de seguridad.
93	Fallas en los registros y definición de acceso a los activos físicos de TI o el uso de dispositivos por parte del usuario para tratamiento de la información.	9	NT	Implementar mecanismos de protección ante la manipulación de información (accesos denegados, bloqueo de puertos y dispositivos) en los diferentes sistemas que puedan ser afectados mediante el uso de dispositivos portátiles.		X			DTIC: Ingeniero 3 Unidad de Centro de Desarrollo de Software, Ingeniero 3 Unidad de Operaciones de Sistemas Informáticos	Coordinador de Sistemas de Información	Número de incidentes que impliquen dispositivos de usuario final. Número de dispositivos de usuario final no autorizados detectados en la red o en el entorno.
		9	NT	Registrar y emplear el uso de tarjetas o placas de identidad previa autorización y supervisión a todos los visitantes de las instalaciones. Y para el personal que labora internamente asegurar que sus perfiles de acceso estén diseñados de acuerdo a sus funciones y responsabilidades.			X		DTIC: Ingeniero 3 de Seguridad CRC, Ingeniero 2 Infraestructura de TI	Coordinador de Redes y Comunicación	Porcentaje de usuarios registrados y entregados tarjetas o placas de autorización para su ingreso a las diferentes áreas administrativas de la universidad. Porcentaje del personal que se actualizado su acceso.
141	Registro de incidentes de seguridad desactualizado lo que imposibilita su evaluación, investigación y retroalimentación.	9	NT	Promover el fácil reconocimiento de los incidentes de seguridad y de sus impactos mediante la comunicación de su naturaleza y características; para luego ser registrados y guardados por un periodo determinado para ser evaluados y empleados en un futuro.	X	X			DTIC: Director de TIC, Ingeniero 3 Unidad de Operaciones de Sistemas Informáticos, Ingeniero 3 de Seguridad CRC	Comisión de Evaluación Interna	Número de incidentes de seguridad causantes de interrupciones del negocio o pérdida de imagen así como también los relacionados con seguridad física.
122	No hay un enfoque hacia la gestión del cumplimiento tanto para objetivos como para su rendimiento.	6	NT	Difundir los objetivos institucionales y de la DTIC para el todo el personal así como también informar de los cambios realizados en los mismos de igual manera anticipar cómo se evaluará su cumplimiento. Se fomentará el uso de informes, circulares o correos electrónicos de fácil comprensión y entendimiento dirigidos desde la alta dirección hacia diferentes destinarios. Se tendrá en cuenta que las evaluaciones del rendimiento se analizarán con el fin de definir el origen de ciertas desviaciones.	X			X	INSTITUCIÓN: Dirección Administrativa, Director General Financiero, Coordinador/a de la Unidad de Relaciones Públicas y Comunicación DTIC: Director de TIC	Rectorado	Porcentaje de informes de rendimiento y supervisión entregados en plazo. Porcentaje de procesos críticos supervisados.

Fuente: Autoras
*Adaptado al Orgánico Funcional de la Universidad de Cuenca

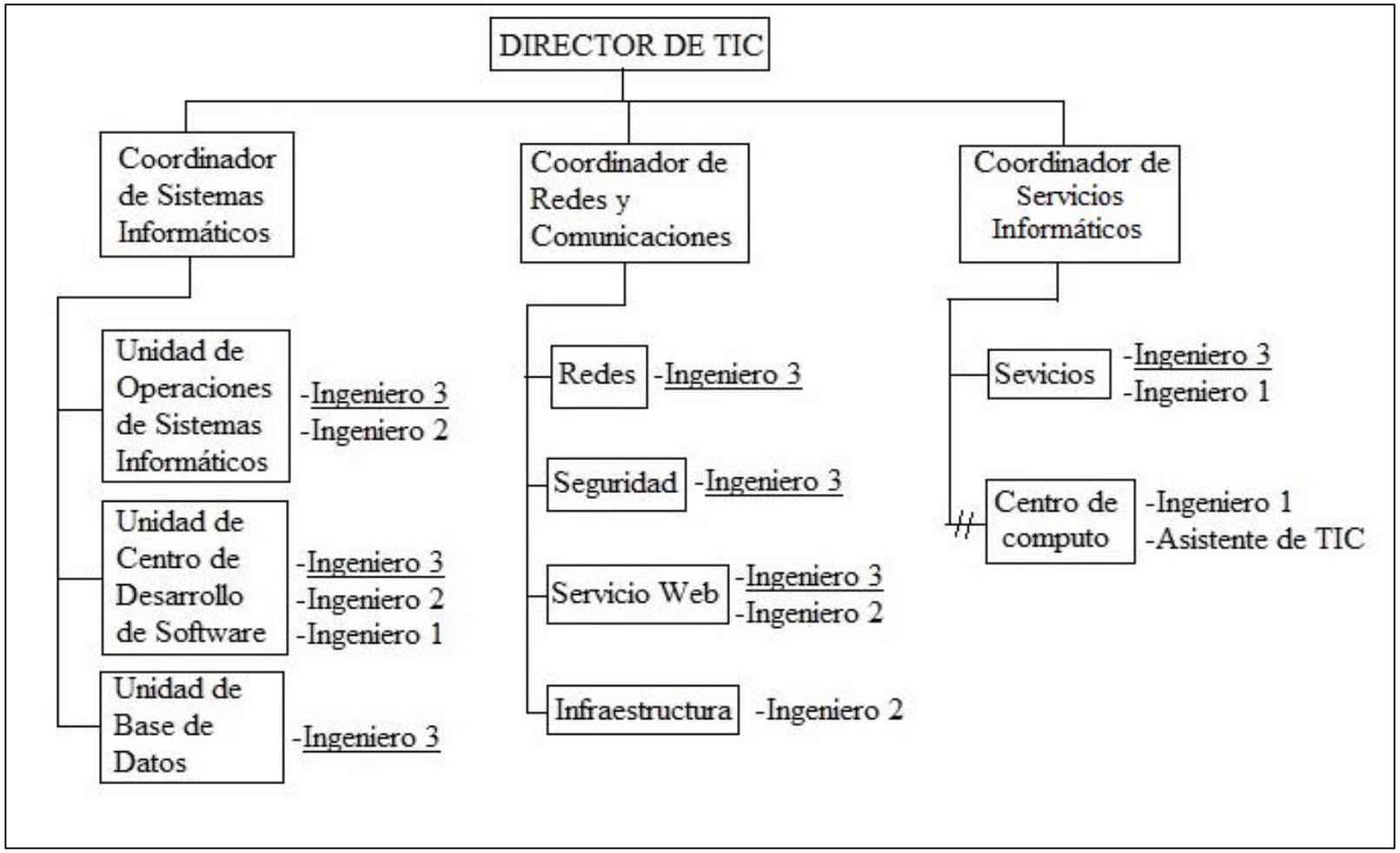
Daisy Fernanda Alvarado Carpio
Laura Alexandra Zumba Morales

Anexo 14: Orgánico Funcional de la Universidad de Cuenca



Fuente: Dirección de Talento Humano de la Universidad de Cuenca

Anexo 15: Organigrama de la DTIC



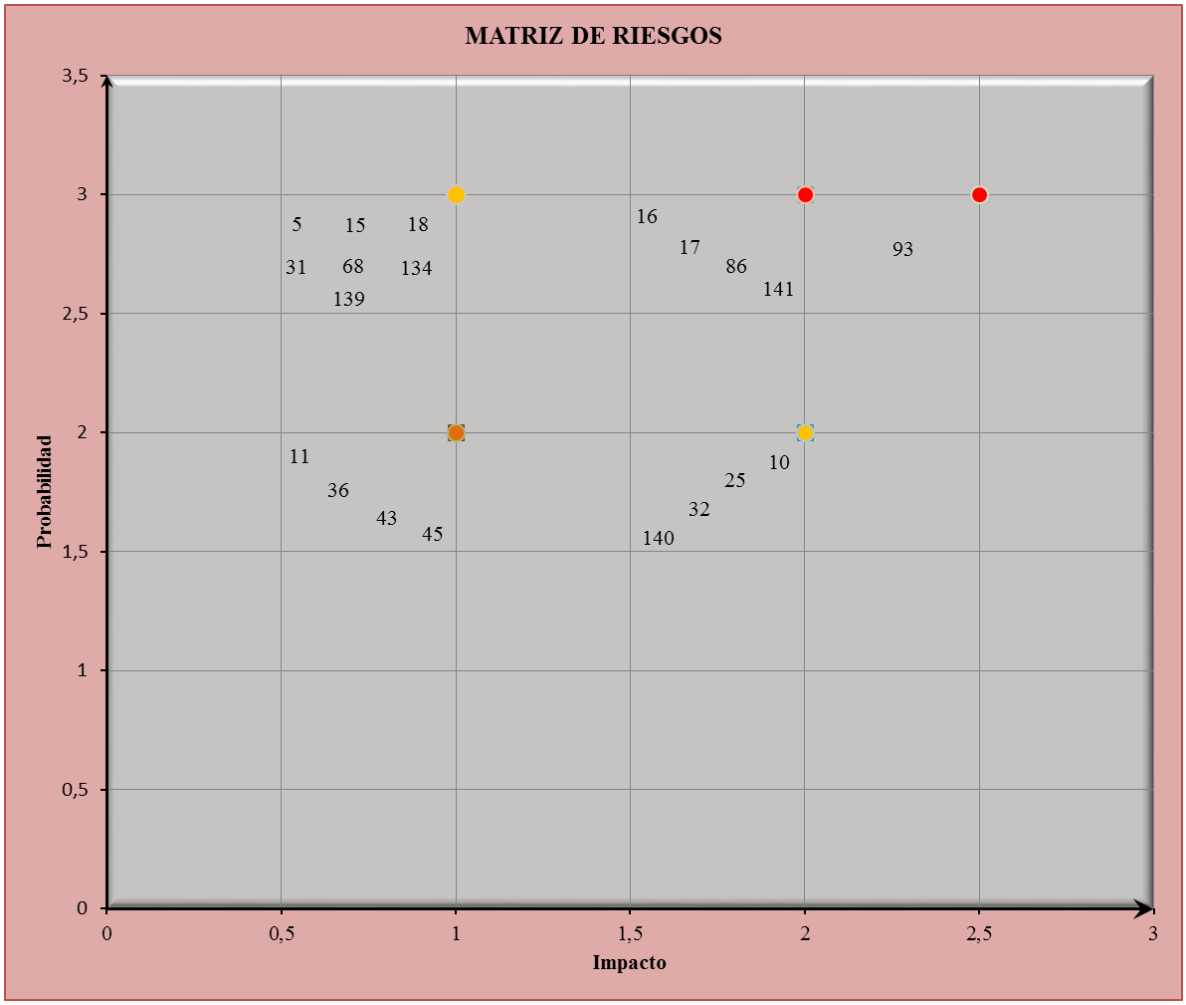
Fuente: Ex - Directora de la DTIC Ing. Carmita Rojas

Anexo 16: Evaluación de Riesgo Residual

N°	RIESGO	NIVEL DE RIESGO		RIESGO RESIDUAL CÁLCULO		
		CUANTITATIVO	CUALITATIVO	Impacto	Probabilidad	Riesgo Residual
86	Ausencia de alineación de las prácticas manejadas en el área de TI con estándares internacionales y códigos de gobierno.	9	NT	2	3	6
45	Ausencia de planes de desarrollo-mejora de habilidades y competencias del personal de TI lo que provoca brechas en las habilidades que poseen estos respecto a las nuevas tecnologías o métodos. (INTERNO)	6	NT	1	2	2
43	Inexistencia de métodos para la evaluación del personal.	6	NT	1	2	2
11	Enfoque desactualizado de la gestión de programas y proyectos.	6	NT	1	2	2
36	Intercambio de información inoportuna e insuficiente con las partes interesadas.	6	NT	1	2	2
15	Planificación inadecuada de los proyectos.	6	NT	1	3	3
16	Deficiencias en la comunicación verbal o escrita adoptada durante el desarrollo del ciclo de vida de un proyecto.	9	NT	2	3	6
17	Ausencia o ineficiencia de un plan de gestión de calidad para los entregables del proyecto	9	NT	2	3	6
18	Ausencia de un proceso para el análisis de riesgo de un proyecto o inefectividad del mismo.	9	NT	1	3	3
25	Desviaciones del rendimiento de los proyectos frente a los requerimientos iniciales y ausencia de un análisis posterior.	6	NT	2	2	4
31	Actividades incompletas sin identificar y comunicar.	6	NT	1	3	3
10	Falta de involucramiento de los usuarios en el ciclo de proyectos, lo que genera un incremento de costes por uso adicional de recursos si existen brechas en las especificaciones o servicios al usuario final.	6	NT	2	2	4
5	Falta de seguimiento y control de las soluciones implementadas.	6	NT	1	3	3
32	Descoordinación en las inversiones importantes relacionadas con TI debido a la falta de comunicación con la alta dirección de la institución, lo que imposibilita el cumplimiento de los objetivos estratégicos planteados.	6	NT	2	2	4
68	Falta de un plan de continuidad que imposibilita responder a incidentes e interrupciones de servicios.	6	NT	1	3	3
134	Ineficiencia o ausencia de dispositivos que detectan las amenazas del entorno, debido a la falta de supervisión, mantenimiento y actualización de los mismos.	9	NT	1	3	3
139	Políticas de prevención y tratamiento de software malicioso desactualizadas o ausencia de las mismas.	6	NT	1	3	3
140	Desactualización de los usuarios respecto a configuraciones de tráfico entrante, uso de correos electrónicos y descargas lo cual facilita el acceso de software malicioso (virus, gusanos, software espía y correo basura).	9	NT	2	2	4
93	Fallas en los registros y definición de acceso a los activos físicos de TI o el uso de dispositivos por parte del usuario para tratamiento de la información.	9	NT	1	3	3
		9	NT	2	3	6
141	Registro de incidentes de seguridad desactualizado lo que imposibilita su evaluación, investigación y retroalimentación.	9	NT	2	3	6
122	No hay un enfoque hacia la gestión del cumplimiento tanto para objetivos como para su rendimiento.	6	NT	2	2	4

Fuente: Autoras

Anexo 17: Matriz de Riesgos Residual



Fuente: Autoras

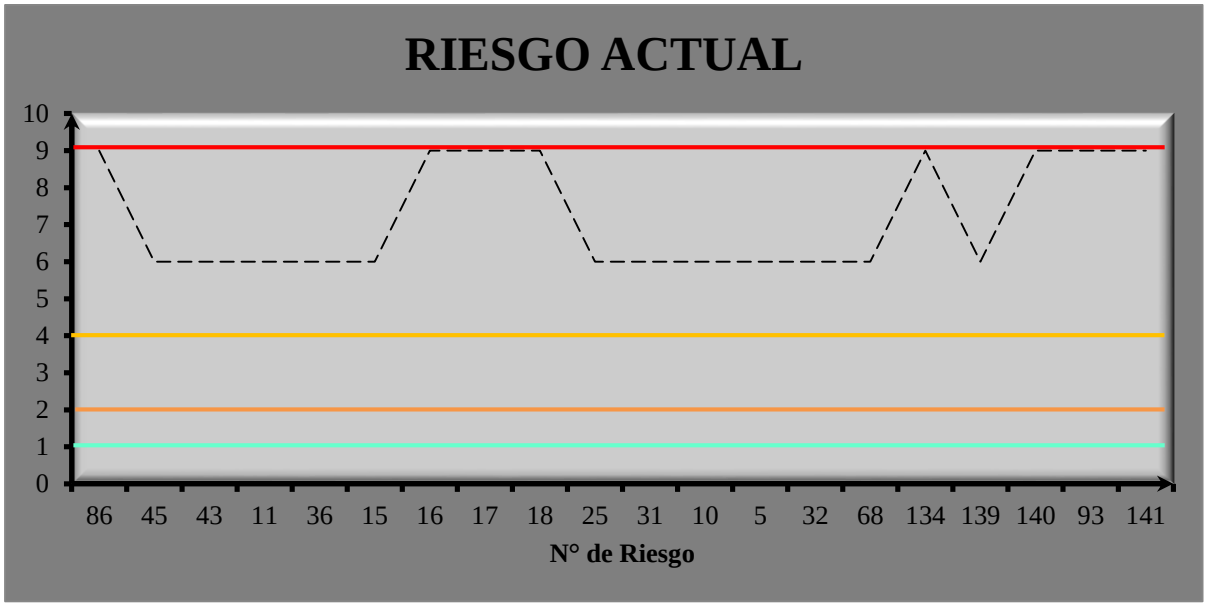
NIVEL DE RIESGO		
COLOR	CALF.	EXPRESIÒN
	6 o 9	Intolerable
	3 o 4	Tolerable
	2	Moderado
	1	Aceptable

Anexo 18: Riesgo Actual vs. Riesgo Residual

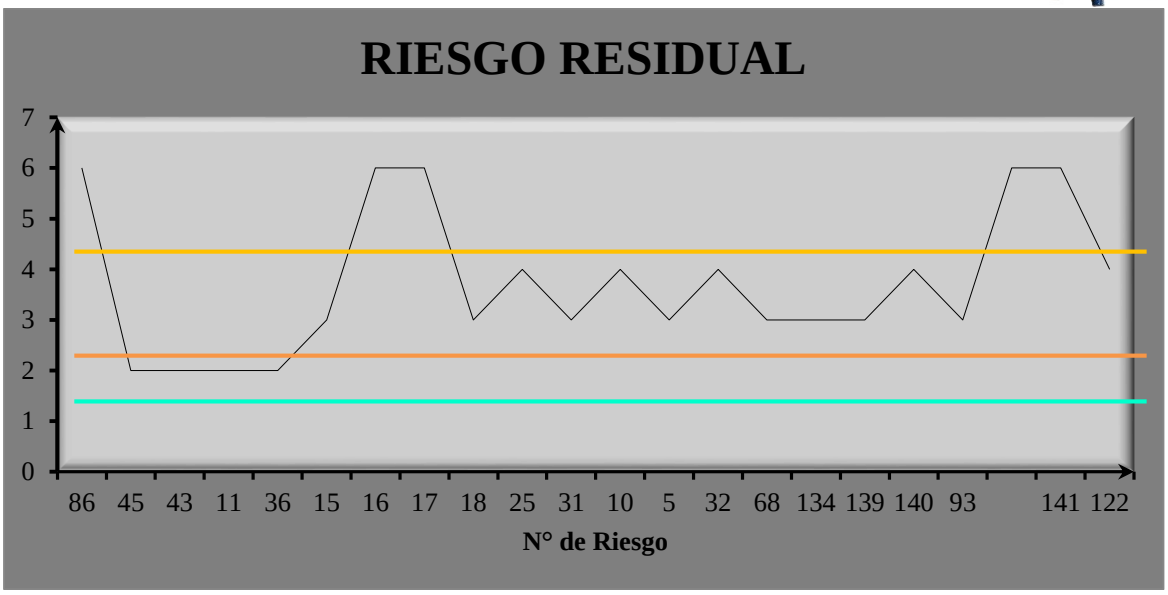
RIESGOS DTIC

N° de Riesgo	RIESGO ACTUAL	RIESGO RESIDUAL
86	9	6
45	6	2
43	6	2
11	6	2
36	6	2
15	6	3
16	9	6
17	9	6
18	9	3
25	6	4
31	6	3
10	6	4
5	6	3
32	6	4
68	6	3
134	9	3
139	6	3
140	9	4
93	9	4,5
141	9	6
122	6	4

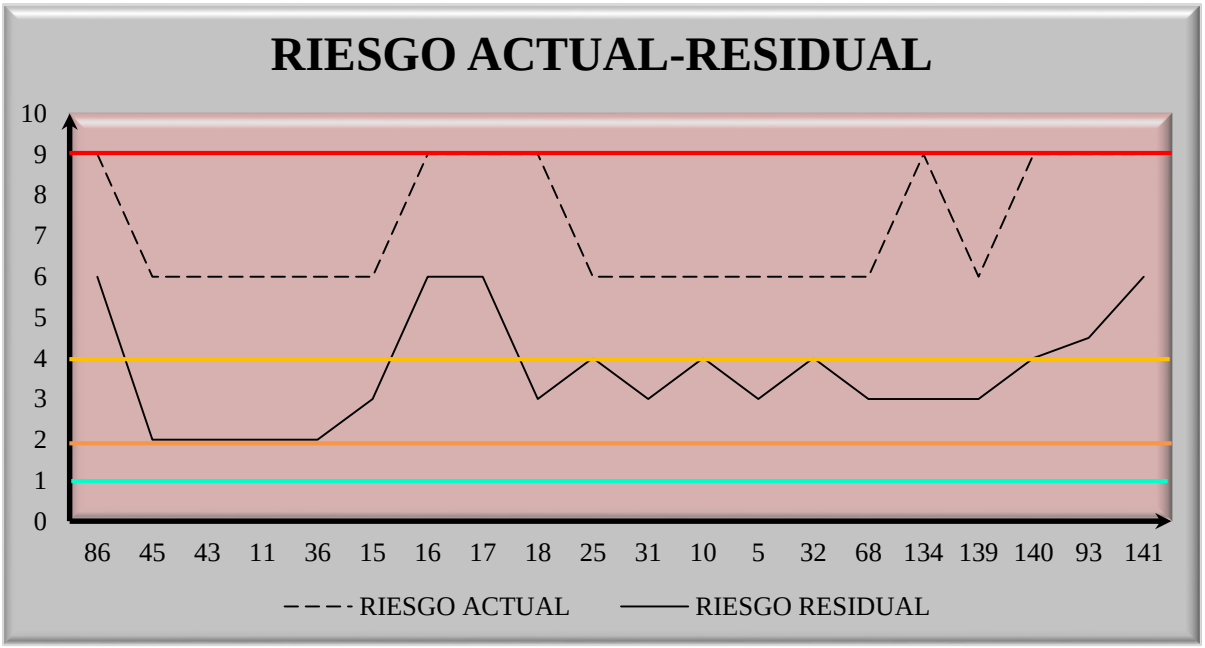
Tabla 1 Valores de Riesgo Actual y Residual
Fuente: Autoras



Fuente: Autoras



Fuente: Autoras



Fuente: Autoras

NIVEL DE RIESGO		
COLOR	**CALF.**	**EXPRESIÒN**
	6 o 9	Intolerable
	3 o 4	Aceptable
	2	Moderado
	1	Tolerable

Anexo 19: Respuesta al Riesgo

N° de Riesgo	RIESGO	RESPUESTA			
		Aceptar	Transferir	Mitigar	Evitar
86	Ausencia de alineación de las prácticas manejadas en el área de TI con estándares internacionales y códigos de gobierno.			X	
45	Ausencia de planes de desarrollo de habilidades y competencias.			X	
43	Inexistencia de métodos para la evaluación del personal.		X		
11	Enfoque desactualizado de la gestión de programas y proyectos.			X	
36	Intercambio de información inoportuna e insuficiente con las partes interesadas.	X			
15	Planificación inadecuada de los proyectos.			X	
16	Deficiencias en la comunicación escrita o verbal adoptado durante el desarrollo del ciclo de vida de un proyecto.			X	
17	Ausencia o ineficiencia de un plan de gestión de calidad para los entregables del proyecto			X	
18	Ausencia de un proceso para el análisis de riesgo de un proyecto o inefectividad del mismo.			X	
25	Desviaciones del rendimiento de los proyectos frente a los requerimientos iniciales y ausencia de un análisis posterior.			X	
31	Actividades incompletas sin identificar y comunicar.			X	
10	Falta de involucramiento de las partes interesadas en el ciclo de proyectos, lo que genera un incremento de costes por uso adicional de recursos si existen brechas en las especificaciones o servicios al usuario final.			X	
5	Falta de seguimiento y control de las soluciones implementadas.			X	
32	Descoordinación en las inversiones importantes relacionadas con TI debido a la falta de comunicación con los altos mandos de la institución, lo que imposibilita el cumplimiento de los objetivos estratégicos planteados.			X	
68	Falta de un plan de continuidad que imposibilita responder a incidentes e interrupciones de servicios.		X		
134	Ineficiencia o ausencia de dispositivos que detectan las amenazas del entorno, debido a la falta de supervisión, mantenimiento y actualización de los mismos.		X		
139	Políticas de prevención y tratamiento de software malicioso desactualizadas o ausencia de las mismas.			X	
140	Desactualización de los usuarios respecto a configuraciones de tráfico entrante, uso de correos electrónicos y descargas lo cual facilita el acceso de software malicioso (virus, gusanos, software espía y correo basura).			X	
93	Fallas en los registros y definición de acceso a los activos físicos de TI o el uso de dispositivos por parte del usuario para tratamiento de la información.			X	
141	Registro de incidentes de seguridad desactualizado lo que imposibilita su evaluación, investigación y retroalimentación.			X	
22	No hay un enfoque hacia la gestión del rendimiento.			X	

Fuente: Autoras

BIBLIOGRAFÍA

Libros

Deloitte; Valero, Nelson; Roa, Mauricio;. (Julio de 2013).

DTIC, Ingeniero de Sistemas. (2014). *Políticas de Tecnología, Marco General de Operación de la Universidad de Cuenca.* Cuenca: Propia.

International Organization for Standardization. (2009). *ISO31000: Gestión de Riesgos - Principios y Directrices.* Suiza: Propia.

Instituto Colombiano de Normas Técnicas y Certificación. (2009). *Proyecto de Norma Técnica Colombiana NTC-ISO 27005.* Bogotá: Propia.

ISACA. (2012). *Un marco de negocio para el gobiero y la gestión de las TI de la empresa .* Estados Unidos: ISBN.

ISACA. (2013). *COBIT for Risk.* Estados Unidos: ISBN.

IT Governace Institute. (2001). *Reunión Informativa del Consejo sobre la Gobernabilidad TI (3ra. Edición).* Mexico.

Mejía, R. C. (2006). *Administración de Riesgos un Enfoque Empresarial, 1ra Edición.* Colombia: Universidad EAFIT.

PwC. (2013). *Control Interno-Marco Regulador: Resumen Ejecutivo.* España.

Valle, J. V. (2012). *Riesgo Tecnológico, Impacto y Autoevaluación en el Negocio.* Panamá: Intendencia de Valores.

Normativa

Constituyente, A. N. (2008). *Constitución de la República del Ecuador 2008.* Quito: Norma.

Contraloría General del Estado. (2009). Norma 410: Tecnología de la Información. En C. G. Estado, *Normas de Control Interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos.* (págs. 73-83). Quito, Distrito Metropolitano.

Sitios Web

Abogados Portaley. (24 de 03 de 2015). *COntrato Informáticos*. Obtenido de http://www.contratosinformaticos.com/sla/

AwE. (2014 de 03 de 24). *AwE Gestión y Desarrollo*. Obtenido de www.ldmatto.com: https://sites.google.com/a/ldmatto.com/awe/arquitectura-de-procesos-1

Be. (24 de 03 de 2015). *Banco de Experiencias*. Obtenido de http://www.planandino.org/bancoBP/node/3

Chanocua, I. P. (4 de Diciembre de 2014). *Fundamentos de Gestión de Servicios de TI*. Obtenido de http://fundamentosdegestiondeserviciosdeti.blogspot.com/2014/12/marcos-de-referencia-para-la-gestion-de_4.html

Comparex. (03 de 24 de 2015). *Comparex*. Obtenido de http://www.comparex-group.com/web/es/es/topics/it-infrastructure/main.htm

Cruz, L. (28 de Septiembre de 2014). *Gestión y Auditoría de TI.* Obtenido de http://gestionyauditoriati.com/2012/08/27/el-riesgo-operativo-y-tecnologico/

David, F. R. (28 de Septiembre de 2014). *Shideshare.* Obtenido de http://es.slideshare.net/anthoanaguilar/conceptos-de-administracion-estrategica-9na-ed-fred-r-david

DNV-GL. (02 de 04 de 2015). *DNV-GL*. Obtenido de http://www.dnvba.com/es/Certificacion/Pages/Por-que-implantar-un-sistema-de-gestion.aspx

García, F. (20 de 02 de 2008). *ORACLE RAC NOTES*. Obtenido de https://oracleracnotes.wordpress.com/2008/02/20/que-es-un-cluster/

International Organization for Standardization. (22 de Abril de 2015). ISO. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en

Martínez, A. F., & Largo, F. L. (22 de Septiembre de 2014). *Conferencia de Rectores de la Universidades Españolas.* Obtenido de http://www.crue.org/Publicaciones/Documents/Gobierno%20TI/gobierno_de_las_TI_para_universidades.pdf

Nakamura, J. M. (12 de 04 de 2015). *SG Buzz*. Obtenido de http://sg.com.mx/buzz/diferencia-entre-programas-proyectos-y-portafolios#.VSrn-NyG9c8

RAE. (2015 de 03 de 2015). *Real Academia Española*. Obtenido de http://lema.rae.es/drae/?val=contingencia

Symantec. (28 de Septiembre de 2014). *Symantec. Confianza en un mundo conectado*. Obtenido de Glosario de Seguridad: http://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad

Varios. (28 de Septiembre de 2014). *Alegsa*. Obtenido de Diccionarios de Informátic y Tecnología: http://www.alegsa.com.ar/Dic/tecnologias%20de%20la%20informacion.php

Varios. (2014 de 03 de 2015). *Definición de*. Obtenido de http://definicion.de/cadena-de-valor/

DISEÑO DE TESIS

1. SELECCIÓN Y DELIMITACION DEL TEMA DE INVESTIGACIÓN

Las TI se han convertido en parte fundamental en el desarrollo de las actividades de una entidad con o sin fines de lucro, ya que representan una ventaja competitiva que pueden llevar al incremento de la productividad, ganar reputación y confianza siempre que las mismas sean adecuadamente manejadas y ocupen un lugar privilegiado dentro de la estructura organizativa; jugando así un papel de asesor de la administración ejecutiva o gerencia pero valiéndose de la información de los niveles inferiores.

En las TI encontramos la materia prima que se necesita en el proceso de toma de decisiones efectivas, *la información,* que a través de su gestión podrá ser de gran utilidad para el alcance de futuras metas así como también un mantenimiento a largo plazo. Por ello se debe tratar a la misma como un activo que necesita de vigilancia y protección continua para asegurar que ésta no sufre pérdidas o es utilizada por agentes externos para fines adversos.

Mediante la realización del presente, la Universidad de Cuenca, institución educativa de gran prestigio a nivel nacional con proyecciones y reconocimiento a nivel internacional, podrá adoptar una metodología para la gestión de riesgos, la misma que le ayudará al cumplimiento de los requerimientos de la Contraloría General del Estado, esto engloba poseer un plan de respuesta a los riesgos, pudiendo así asignar roles críticos para administrar los riesgos de tecnología de información, escenarios de contingencias así como también la responsabilidad respecto de la seguridad de la información, lo que permitirá incrementar su confidencialidad así como la integridad y disponibilidad de la información cuando sea oportuno.

DELIMITACIÓN:

Contenido: Auditoría de sistemas
Área: Gestión de Riesgos, basado en el marco estándar COBIT 5
Organización: Universidad de Cuenca
Temporalidad: Periodo 2014

Bajo este contexto nuestro tema de investigación queda estructurado de la siguiente manera: ***Elaborar un Plan de Gestión de Riesgos de Tecnología de la Información y Comunicación basado en el Marco COBIT 5 para Riesgos aplicado a la Universidad de Cuenca.***

2. JUSTIFICACIÓN DE LA INVESTIGACIÓN

Actualmente el riesgo al cual se encuentra expuesta la Universidad de Cuenca es el riesgo tecnológico y seguridad informática, estos se contemplan dentro del riesgo sistémico y operativo, ya que no posee un plan para la mitigación de riesgos de TI. En la ejecución de los proyectos de tecnologías informáticas no se evalúan permanentemente los riesgos identificados por consiguiente no se registra su evolución de manera que no existe retroalimentación para futuros proyectos.

Se ha considerado realizar este análisis, debido a que la institución requiere un adecuado y oportuno control de la gestión de riesgos de la tecnología de la información, lo cual se podrá mejorar a través del desarrollo de la presente tesis, que le permitirá al Gobierno de TI de la Universidad de Cuenca conectar los riesgos del negocio con las necesidades de control de la institución mediante la *metodología para la gestión de riesgos de TIC basada en COBIT 5 para riesgos,* logrando así beneficios del Gobierno de TI lo que fomentará a una administración adecuada de los recursos de TI, teniendo en cuenta la optimización de recursos y costos derivados.

El Gobierno de TI es parte de un gobierno corporativo, por lo tanto define los derechos y las responsabilidades de las partes relacionadas, necesarios para la consecución de la misión y visión fijada por la institución y todo lo que ello engloba. Las TI también son gobernadas por mejores prácticas que aseguran que la información generada en la organización y las tecnologías relacionadas apoyan los objetivos de la entidad, dentro de estas podemos considerar: ITIL, ISO 27001-27002, PMBOK, PRINCE y el marco de apoyo seleccionado para el presente trabajo COBIT 5. El uso de esta tecnología trae consigo riesgos y por ende una pregunta que toda entidad debe hacerse ¿se está gestionando estos riesgos?

La Universidad de Cuenca está regulada por el Estado y se encuentra sujeta al cumplimiento de las Normas de Control Interno dentro de las cuales se considera

a las Tecnologías de la Información (Norma 410: TI), en la que se especifica la forma de crear las condiciones necesarias para ejercer control, se menciona (Norma 410-04: Políticas y Procedimientos) lo siguiente: "*Temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, serán considerados dentro de las políticas y procedimientos a definir, los cuales además, estarán alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información*" (Contraloría General del Estado, 2009).

Emplear una gestión de riesgo permite detectar, prevenir y reaccionar ante los eventos que pueden exponer a peligros o representar pérdidas de oportunidad en cuatro ámbitos diferentes: estratégico y operativo, de seguridad, de fiabilidad y disponibilidad de la información, y de cumplimiento de la legislación y regulación normativa. Una vez detectados los riesgos se priorizan y generan planes de respuesta para estos. Es así que la institución podrá identificar oportunidades pero también amenazas, con lo cual se podrá evitar o mitigar las pérdidas económicas y la imagen asociada, se proveerá de pautas para que las decisiones respecto a las acciones necesarias como respuesta a las amenazas detectadas no sean improvisadas ni tardías sino que se encuentren debidamente planificadas y sean oportunas.

Todo ello conllevará a que la institución tenga un mejoramiento sistemático en el desarrollo de sus actividades a través del alineamiento de los objetivos de las TI con los objetivos de la institución, evitando el uso inadecuado de sus recursos, así como también asegurar la continuidad operacional de la institución y justificar una mejora continua de la seguridad de la información, que permita minimizar el impacto, con reducción de costos, que incluyen: pérdidas de dinero, tiempo y mano de obra.

A nivel personal, este análisis permitirá profundizar y aplicar a la realidad temas aprendidos en las aulas de la materia de Auditoría de Sistemas, relacionando el manejo, control y aplicación de las pautas que se deben seguir para que el uso y administración de las TI sea eficiente mediante la aplicación de COBIT 5 para Riesgos, generando así un mayor conocimiento y proyecciones de nuestros

potenciales campos de trabajo, así como también brindar un aporte a la gestión actual de nuestra universidad.

3. BREVE DESCRIPCIÓN DEL OBJETO DE ESTUDIO

La Universidad de Cuenca fue fundada por decreto legislativo el 15 de octubre de 1867, tiene una antigüedad de 147 años, es una institución educativa de tercer y cuarto nivel con sede en la ciudad de Cuenca provincia del Azuay, a su vez cabecera de la región centro-sur del Ecuador. Entidad educativa pública que brinda excelencia educativa en el campo profesional generando por décadas un alto número de egresados con los más altos perfiles competitivos.

La Universidad de Cuenca es una institución del Estado, cuya misión es formar profesionales y científicos comprometidos con el mejoramiento de la calidad de vida, en el contexto de la interculturalidad y en armonía con la naturaleza. La Universidad se fundamenta en la calidad académica, en la creatividad y en la innovación, su capacidad para responder a los retos científicos y humanos de la época y sociedad regional, nacional e internacional equitativa, solidaria y eficiente.

Por otra parte, la misma se proyecta como una institución con reconocimiento nacional e internacional por su excelencia en docencia con investigación y vinculación con la colectividad; comprometida con los planes de desarrollo regional y nacional; que impulsa y lidera un modelo de pensamiento crítico en la sociedad.

Posee una Dirección de Postgrado que organiza las políticas académicas de cuarto nivel, y un Departamento de Desarrollo Informático a cargo de la capacitación y aplicación de tecnologías de la información (TI) para avanzar en los procesos de administración y gestión generados en dicha área proporcionando seguridad, disponibilidad y oportunidad en la misma a fin de satisfacer las necesidades de las partes interesadas.

4. FORMULACIÓN DEL PROBLEMA

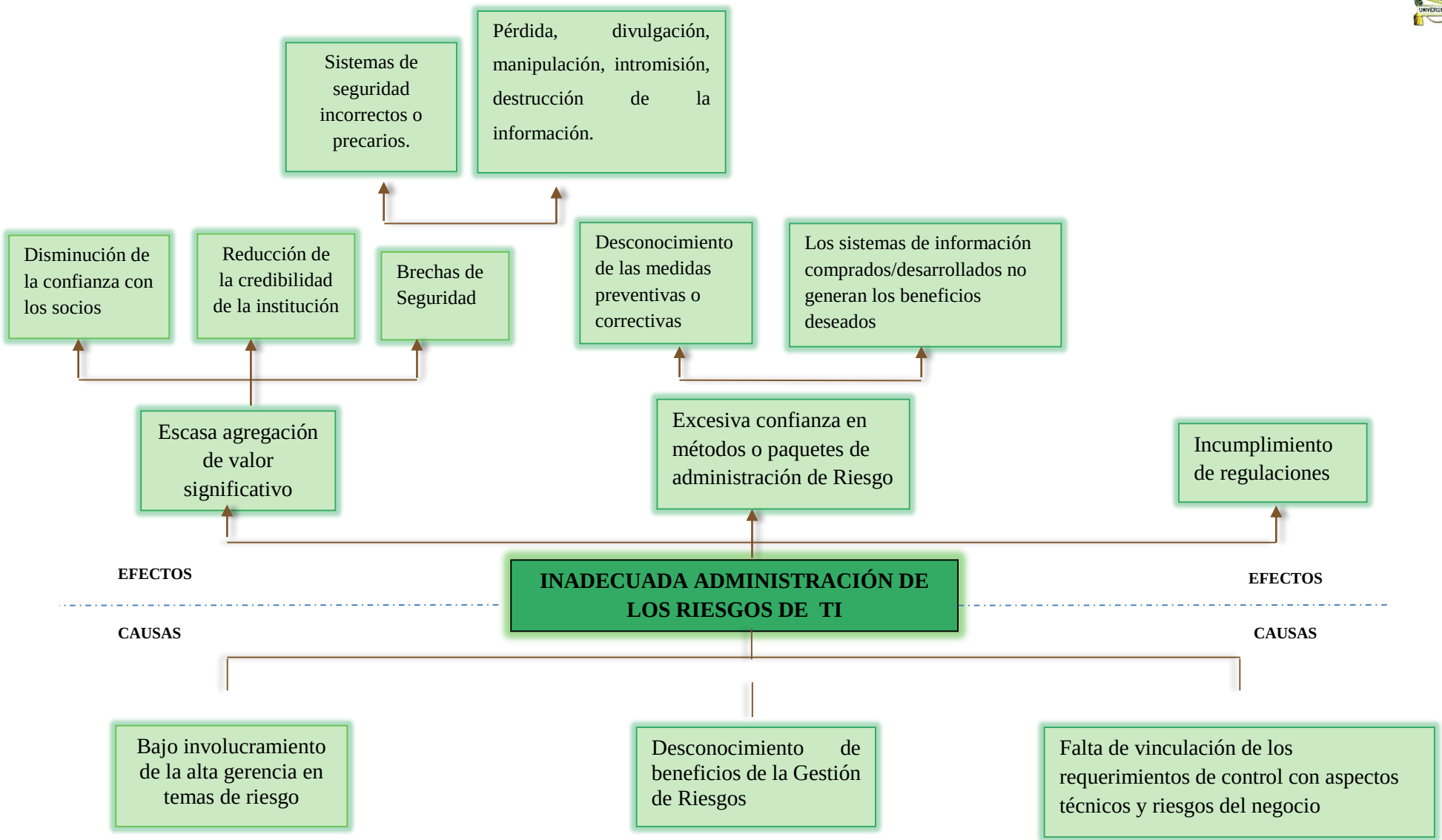
Debido a la globalización, en un mundo cada día más complejo la tecnología se ha convertido en algo transcendental y de vital importancia dentro de las instituciones es por ello que se requiere una adecuada gestión de riesgos de

tecnologías de información porque ayuda a generar una ventaja competitiva, aún más dentro de una entidad educativa donde la información tanto tangible como intangible requiere un tratamiento de igual o mayor nivel que el resto de áreas.

Es desconcertante saber que al obviar la importancia del área de TI así como la gestión de riesgos, la institución puede incurrir en problemas tales como: un desordenado crecimiento tecnológico, inversiones innecesarias o mal aprovechadas y la insuficiencia de una visión tecnológica. La falta de protección de activos de TI críticos provocan que la institución está expuesta tanto a vulnerabilidades como posibles amenazas que alteren el funcionamiento de la misma ocasionando: pérdida, divulgación, manipulación, intromisión y destrucción de la información.

Por el escenario antes mencionado, le imposibilita al crecimiento de una manera adecuada, tener organizada e integrada la infraestructura de TI, aun cuando la mayoría de los procesos de negocio son planteados en los planes trimestrales de esta forma se hace evidente los riesgos a los cuales se encuentran expuestos. En cuanto a la protección de activos se debe tener conciencia que esta no implica acciones únicamente físicas tales como la colocación de equipos en espacios seguros sino también acciones de aspectos que se relacionen con la lógica de estos, que permita cubrir desde los aspectos básicos a nivel de conectividad de red, protección contra ataques, admisión exclusiva del tráfico de servicio, protección a nivel de aplicaciones entre otras.

Por ende la no identificación de los riesgos que afectan al área de TI mediante la oportuna comparación del marco de Referencia COBIT 5 y las Normas de Control Interno establecidas por la Contraloría General del Estado, impide la identificación de los procesos que poseen riesgos significativos para lograr el establecimiento de medidas de mitigación de acuerdo a su naturaleza.



Daisy Fernanda Alvarado Carpio
Laura Alexandra Zumba Morales

5. DETERMINACIÓN DE LOS OBJETIVOS

5.1 OBJETIVO PRINCIPAL

Elaborar un Plan de Gestión de Riesgos de las Tecnologías de Información y Comunicación basado en el Marco COBIT 5 para Riesgos de manera que los riesgos identificados sean tratados de manera adecuada.

5.2 OBJETIVOS ESPECÍFICOS

1) Analizar cómo se encuentran definidos los planes, estructura y procesos desarrollados en el área de TI de la Universidad de Cuenca para establecer la alineación entre el plan estratégico institucional y el plan estratégico de TI.
2) Entender el marco regulatorio interno y externo de la entidad relacionándola con estatutos, reglamentos y normas legales vigentes.
3) Analizar las mejores prácticas y estándares de tecnología de información a emplear por el gobierno TI para agregar valor en cuanto a la eficiencia en la administración de la gestión de riesgos de la institución.
4) Desarrollar el proceso de gestión de riesgos a través de las etapas de recopilación de datos, análisis, mantención de un portafolio de riesgos, expresión del riesgo, definición de un portafolio de acciones y respuesta a los riesgos más significativos.

6. ELABORACIÓN DEL MARCO TEORICO DE REFERENCIA

6.1 MARCO DE ANTECEDENTES

Gobierno de las TI para universidades (Antonio Fernández Martínez; Faraón Llorens Largo)

La gestión de las Tecnologías de la Información (TI) en las universidades españolas tiene como principal propósito lograr una administración eficiente de los recursos tecnológicos como soporte fundamental del resto de servicios universitarios, el mismo que según estudios UNIVERSITIC realizados (Uceda y

otros, 2010), afirma que se está haciendo efectivo en la mayoría de las universidades.

A nivel internacional, son pocas las universidades que hayan llevado a cabo implantaciones de gobierno de las TI, bien utilizando COBIT o diseñando modelos propios. Algunas de ellas se encuentran aplicando COBIT, como por ejemplo South Louisiana Community Collage. (Martínez & Largo, 2014)

El 55% de las universidades informan sobre la utilización de alguna herramienta (COBIT, ITIL, estándares ISO, etc.) como soporte a los sistemas de gobierno de las TI, aunque ninguna de estas herramientas presenta una amplia utilización y cuando se utilizan se hace de manera selectiva (sólo para algunos procesos).

Implementación de COBIT en la Educación Superior: Prácticas que funcionan mejor.

Presenta el estudio de la exploración de los aspectos de la implementación de un modelo de gobierno de las TI de *los Objetivos de Control para la Información y* (COBIT) *Tecnologías Relacionadas* en South Louisiana Community College (SLCC) en Lafayette, Louisiana, EE.UU.

Este se realizó utilizando COBIT 3rd Edition. A lo largo del estudio, se observó la aplicación del proceso de COBIT quinta entrega y el soporte (DS5) perteneciente a la red de seguridad. Esta exploración examinó las necesidades profesionales y personales, ayudo también a fomentar el liderazgo en SLCC para el cumplimiento de sus funciones más básicas detectando comunes problemas tales como la dificultad de los controles de seguridad en las contraseñas y que expiran hacen disminuir la comodidad de autenticación en otros se destaca que las instituciones cuentan con un presupuesto limitado, y estos fondos deben ser priorizadas. Esto pone de relieve la importancia de la presentación de la administración de los riesgos cuantificados en pérdidas potenciales de modo que puedan tomar decisiones informadas sobre qué gastos son apropiados.

Es así, que se demostró que las instituciones medianas de educación superior pueden beneficiarse de la aplicación de un programa de seguridad de Gobierno de TI.

6.2 MARCO TEORICO

NORMAS DE CONTROL INTERNO PARA ENTIDADES, ORGANISMOS DEL SECTOR PÚBLICO Y DE LAS PERSONAS JURÍDICAS DE DERECHO PRIVADO QUE DISPONGAN DE RECURSOS PÚBLICOS. *NCI 410:* TECNOLOGÍA DE LA INFORMACIÓN (Contraloría General del Estado, 2009)

La Contraloría General del estado ente regulador de las instituciones Públicas emitió estas normas de control interno basadas en los componentes del COSO I tales como: Ambiente de Control, Evaluación de Riesgo, Actividades de Control, Comunicación e Información y Seguimiento.

Para el desarrollo del presente tema se enfoca en el componente Actividades de Control dentro de las cuales la norma 410 menciona los lineamentos que deben regir para la TECNOLOGÍA DE LA INFORMACIÓN dentro de la institución para lo cual se deberá tomar en cuenta una adecuada *organización informática* de la cual se establece la *segregación de funciones* que permitan ejercer las actividades con suficiente autoridad y respaldo soportados con un *plan informático estratégico de tecnología* que este en concordancia con el plan estratégico institucional, para lo cual es necesario establecer *políticas y procedimientos,* así como también un *modelo de información organizacional* que delimite el marco de trabajo.

En esta normativa provee mecanismos para la *administración de proyectos tecnológicos* que faciliten su administración, teniendo en cuenta aspectos importantes para el *desarrollo y adquisición de software o infraestructura tecnológica.* Por otra parte se recalca la importancia sobre la *seguridad de la tecnología de la información* dentro de los cuales se toma en cuenta los *planes*

de contingencia, así como la *administración de soporte de tecnología de la información, monitoreo y evaluación de los procesos y servicios.*

Por último, plantea la elaboración de normas, procedimientos e instructivos para manejo de sitio web, servicio de internet e intranet para lo que se necesita una *capacitación informática* y el establecimiento de un *comité informático.*

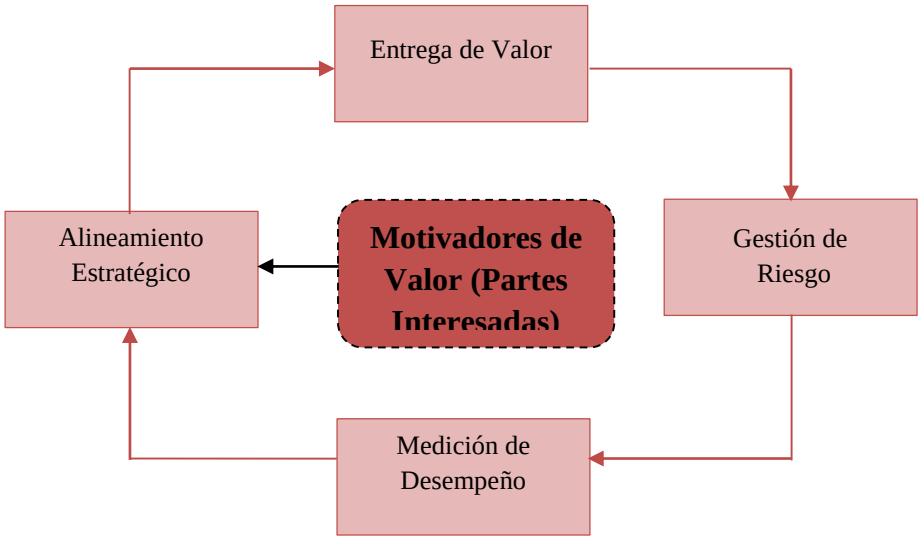
IT GOVERNANCE INSTITUTE (IT Governace Institute, 2001)

El IT Governance Institute (ITGI), fundado por la Information Systems Audit and Control Association (Asociación de Control y Auditoría de Sistemas de Información) y su fundación afiliada en 1998, busca asistir en el liderazgo empresarial para asegurar un éxito constante y duradero junto con un mayor valor del inversionista al ampliar la conciencia acerca de la necesidad y el beneficio de un manejo adecuado de la TI.

El Instituto desarrolla y promueve la comprensión de lo importante que es el vínculo entre la TI y el manejo de una empresa de los riesgos relacionados con la TI.

Postula que un manejo adecuado de TI implica enfocarse en dos puntos clave: la generación de valor y la mitigación de riesgos de TI. Para ello establece las siguientes estructuras de Relaciones del Gobierno de TI[1]:

[1] Tomado de documento entregado por el docente Ing. Paúl Ochoa A. MBA CISA. Capitulo: Gobierno de TI pág.4 con fecha 09-03-2014



Respecto al alineamiento estratégico se menciona la correspondencia y coherencia que debe existir entre los objetivos del negocio y los de TI, alineando entonces POA y PE institucionales con los PETI Y POTI. La entrega de valor se refiere a la entrega de beneficios relacionados con el tiempo así como el presupuesto, para ello se pueden aplicar técnicas de ingeniería o marcos para gestión de proyectos, dependiendo el caso.

La gestión de riesgos se enfoca en anticiparse a la ocurrencia de eventos que destruyan el valor agregado de la institución, para ello se toma en consideración la misión, visión, objetivos y la regulación vigente relacionada al objeto de estudio en el momento de realizar dicho proceso. Finalmente se plantea la necesidad de la medición de desempeño, que se vuelve la única forma de administrar, aquí cabe preguntar ¿Ti está o no alineada a la organización?, para resolver dicha cuestión se recurre al empleo de indicadores. Se aplica la regla de: para administrar debo gestionar y para ello debo medir.

COBIT 5 (ISACA, 2012)

Es un marco de trabajo que ayuda en dos actividades fundamentales relacionadas a las TI, estas son: gobernar y gestionar. No se trata de un lenguaje técnico de compleja aplicación más bien está orientado a los negocios ya que busca que la entidad mantenga una total coherencia entre el Plan Estratégico

Institucional y el Plan Estratégico de TI de manera que se dé la tan necesaria creación de valor. Forma parte de una gran variedad de estándares reconocidos y aceptados globalmente, como son: ISO 27000, COSO ERM, ISO 9001, ISO 31000, PMBOK, CMMI, etc., mismos que se usan como herramienta por auditores y administradores de negocios.

No se enfoca sólo en el área de TI, al contrario, actúa a lo largo de todas las actividades que contempla la entidad teniendo en cuenta los intereses de todas y cada una de las partes interesadas. Este modelo es versátil y adaptable a cualquier empresa sea esta del sector público o privado así como con o sin ánimos de lucro. Se basa en cinco principios claves para gobernar y gestionar las TI en los que se basa la consecución de metas institucionales apoyadas en la aplicación de siete catalizadores.

COBIT 5 PARA RIESGOS (ISACA, 2013)

Forma parte de la familia de productos de COBIT 5, se trata de una guía profesional que presenta dos perspectivas de cómo usar COBIT 5 en un contexto de riesgos. La primera perspectiva es de la función del riesgo que describe cómo construir y sostener una función de riesgo en la empresa usando los catalizadores de COBIT 5. La segunda perspectiva se trata de la gestión del riesgo que se enfoca en analizar el núcleo del gobierno de riesgos y el proceso de gestión del riesgo así como los escenarios de riesgo.

Esta herramienta permite que se logre un mejor entendimiento sobre el impacto de los riesgos de TI a nivel de toda la institución ya que es una guía de extremo a extremo para la forma de gestionar los mismos. Se basa en dos procesos claves que apoyan la perspectiva de la gestión de riesgos:

- EDM03 (Asegurar la optimización del riesgo): Proceso que permite asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.

- APO12 (Gestionar el riesgo): Proceso que permite identificar, evaluar y reducir los riesgos relacionados a las TI de forma continua, dentro de los niveles de tolerancia establecidos por la dirección ejecutiva de la entidad.

6.3 MARCO CONCEPTUAL

Alineamiento: Un estado en el que los elementos facilitadores del gobierno y la gestión de TI de la entidad contribuyen a las metas y estrategias de la misma. (ISACA, 2013)

Amenaza: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio. (ISACA, 2013)

Catalizadores: Cualquier inversión que está siendo considerada y/o realizada que permita alcanzar los objetivos de la empresa. (ISACA, 2013)

Creación de valor: Es el objetivo principal del gobierno de una empresa, se consigue cuando existe equilibrio entre: la consecución de objetivos, optimización de riesgos y optimización de recursos. (IT Governace Institute, 2001)

Escenarios de riesgo: Es una descripción de un posible caso de que, cuando se produzca, tendrá un impacto incierto en el logro de los objetivos de la empresa. El impacto puede ser positivo o negativo. (ISACA, 2013)

Gestión: Incluye el uso juicioso de medios (recursos, personas, procesos, prácticas, etc.) para conseguir un fin identificado. Es un medio o instrumento mediante el cual el grupo que gobierna consigue un resultado u objetivo. (ISACA, 2013)

Gestión de Riesgos: Constituye uno de los objetivos del gobierno. Requiere conocer un riesgo; evaluar su impacto y su probabilidad; desarrollar estrategias, como, por ejemplo: evitar el riesgo, reduciendo el efecto negativo de riesgo y/o

transfiriendo el riesgo, para gestionarlo en el contexto del apetito de riesgo de una entidad. (ISACA, 2012)

Gobierno corporativo.- Se define como un comportamiento corporativo ético por parte de los directores u otros encargados del gobierno, para la creación y entrega de los beneficios para las partes interesadas. (IT Governace Institute, 2001)

Mejores prácticas.- Actividades o procesos probados que se han utilizado con éxito por varias organizaciones. ITIL es un ejemplo de buenas prácticas. (IT Governace Institute, 2001)

Objetivos: Metas hacia donde se deben enfocar los esfuerzos y recursos de la empresa, se definen como resultados específicos que una empresa intenta lograr para cumplir con su misión básica. (David, 2014)

Políticas: Son los medios por los cuales se logran los objetivos anuales. Las políticas incluyen directrices, reglas y procedimientos establecidos con el propósito de apoyar los esfuerzos para lograr los objetivos establecidos. (David, 2014)

Principio: Comprende los valores y las hipótesis fundamentales contenidas en la empresa, las creencias que la guían y que definen sus límites entorno a los procesos de decisión, comunicación interna o externa y la administración.

Proceso: Generalmente una colección de prácticas influenciadas por las políticas y procedimientos de la empresa que toma entradas de una serie de fuentes (incluyendo otros procesos), manipula esas entradas y genera salidas (por ejemplo: productos y servicios). (ISACA, 2012)

Riesgo: La combinación de la probabilidad de un evento y sus consecuencias. (ISACA, 2013)

Riesgo operativo: El riesgo operativo se refiere a la probabilidad de que una empresa incurra en pérdidas financieras por la interrupción de sus operaciones,

debido a fallas en los procesos, las personas, las causas naturales, los siniestros y la fallas de sistemas de información. (Cruz, 2014)

Riesgo tecnológico.- se refiere a la probabilidad de que los servicios de TI no alcancen los niveles de servicio requeridos para soportar las operaciones de una empresa e impacten en los resultados. (Cruz, 2014)

Riesgo de TI.- Es el riesgo de negocio asociado con el uso, propiedad, operación, involucramiento, influencia y adopción de la TI dentro de la empresa. Este riesgo consiste en los eventos relacionados con la TI que pueden potencialmente impactar al negocio. (Symantec, 2014)

TI: Tecnologías de la información o simplemente TI, es un amplio concepto que abarca todo lo relacionado a la conversión, almacenamiento, protección, procesamiento y transmisión de la información. El concepto se emplea para englobar cualquier tecnología que permite administrar y comunicar información. (Varios, Alegsa, 2014)

Vulnerabilidad: Es una debilidad en el diseño, implementación, operación o control interno de un proceso que podría exponer al sistema a ciertas amenazas o eventos adversos. (ISACA, 2013)

7. DISEÑO METODOLÓGICO

a) Tipo de investigación

El presente trabajo se basa en una investigación de tipo descriptiva-aplicativa, a través de la cual se conocerá la forma de operar y las características de los diversos procesos de negocio del área de TI; dando paso a la realización de la metodología para la identificación y conocimiento de los principales riesgos que se puedan presentar en estos.

b) Método de la investigación

La investigación se la realizará a través del método inductivo (cualitativo), ya que nos enfocaremos tanto en los manuales, planes estratégicos, políticas y

procedimientos utilizados por la Universidad los cuales plasman como se lograrán los objetivos institucionales; así como también en la Norma de Control Interno que es de cumplimiento obligatorio por esta NCI°410 (TI), para esto se incurrirá a la observación y la indagación generando así la constatación de dicho cumplimiento tanto de la normativa interna como externa y el levantamiento de las vulnerabilidades a las cuales está sujeta.

También se considera necesario realizar una entrevista dirigida con personal calve del área a la cual se aplica el tema de manera que se consiga información relevante y objetiva.

c) Modalidad de la investigación

En cuanto a la modalidad se considera el aspecto cualitativo pues se explorará el problema a profundidad de lo cual se obtendrá significados profundos de los datos explorados dentro del área en cuestión.

8. ESQUEMA TENTATIVO DE LA INVESTIGACION

CAPÍTULO I: INFORMACIÓN INSTITUCIONAL

1.1. Introducción
1.1.1. Misión
1.1.2. Visión
1.1.3. Valores
1.2. Objetivos Institucionales
1.3. Estructura Organizacional
1.4. Departamento de Desarrollo Informático
1.4.2. Misión
1.4.3. Objetivos de la DTIC
1.4.4. Funciones
1.5. Plan Estratégico
1.5.1. Plan Estratégico Institucional
1.5.1.1. Marco Legal
1.5.1.2. Objetivos Estratégicos de Desarrollo Institucional

1.5.2. Plan Operativo Anual 2014 de la Dirección de Tecnologías de Información y Comunicación

CAPÍTULO II: MARCO REGULADOR

2.1. Antecedentes

2.2. Marco Interno

2.2.1. Estatuto

2.2.2. Política de TI

2.3. Marco externo

2.3.1.1. Misión

2.3.1.2. Visión

2.3.1.3. Funciones

2.3.2. Normas de Control Interno para entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos.

2.4. COSO

2.4.1. Control Interno

2.4.2. Componentes del CI

CAPÍTULO III MEJORES PRÁCTICAS

3.1. Antecedentes

3.2. ISO 31000: Gestión de Riesgos - Principios y Directrices

3.2.1. Antecedentes

3.2.2. Principios

3.2.3. Marco de referencia

3.2.4. Procesos

3.2.4.1. Establecer un contexto

3.2.4.2. Valoración del Riesgo

3.2.4.3. Tratamiento del Riesgo

3.2.4.4. Monitoreo y revisión

3.2.4.5. Comunicación y consulta

3.3. ISO 27005: Gestión del Riesgo en la Seguridad de la Información

9. CRONOGRAMA DE ACTIVIDADES

ACTIVIDADES	MES	SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE				ENERO				FEBRERO				MARZO			
	SEM	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Presentación del tema																													
Aprobación del tema																													
Diseño de Tesis																													
Aprobación diseño de tesis																													
Capítulo 1: *Información de la Institución*																													
Revisión del director de tesis																													
Correcciones y aprobación																													
Capítulo 2: *Marco Regulatorio*																													
Revisión del director de tesis																													
Correcciones y aprobación																													
Capítulo 3: *Estándares y Marco de Referencia*																													
Revisión del director de tesis																													
Correcciones y aprobación																													
Capítulo 4: *Metodología para la gestión de Riesgo*																													
Revisión del director de tesis																													
Correcciones y aprobación																													
Conclusiones y Recomendaciones																													
Bibliografía																													
Anexos																													
Correcciones y aprobación																													
Encuadernación y presentación de tesis																													

10. PRESUPUESTO DE ACTIVIDADES

PRESUPUESTO REFERENCIAL							
CONCEPTO	OCTUBRE	NOVIEMBRE	DICIEMBRE	ENERO	FEBRERO	MARZO	VALOR TOTAL
Materiales de Oficina	$ 3	$ 2		$ 2		$ 3	$ 10
Internet	$ 25	$ 25	$ 25	$ 25	$ 25	$ 25	$ 150
Movilización		$ 5	$ 5	$ 5	$ 10	$ 10	$ 35
Impresiones	$ 10	10				$ 220	$ 240
Copias de libros, artículos, etc.	$ 20	$ 20			$ 10		$ 50
Empastado					$ 30		$ 30
					TOTAL		$ 515